INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2016/2017

TII

CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL DE CIBERDEFESA

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Luís Filipe Camelo Duarte Santos

Coronel de Transmissões

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL DE CIBERDEFESA

COR TM Luís Filipe Camelo Duarte Santos

Trabalho de Investigação Individual do CPOG

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL DE CIBERDEFESA

COR TM Luís Filipe Camelo Duarte Santos

Trabalho de Investigação Individual do CPOG

Orientador: COR TIR CAV Vítor Manuel Meireles dos Santos

Pedrouços 2017

Declaração de compromisso antiplágio

Eu, **Luís Filipe Camelo Duarte Santos**, declaro por minha honra que o documento intitulado "**Contributos para uma estratégia nacional de ciberdefesa**" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial General 2016/2017** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência de que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 02 de maio de 2017

Agradecimentos

Ao meu orientador e às entidades entrevistadas,
pelo inestimável tempo dispensado.

Ao Coronel Tirocinado Pereira dos Santos,
pela disponibilidade demonstrada.

Ao Exército,
pelas oportunidades de conhecimento que me proporcionou.

Aos meus camaradas auditores,
pelo extraordinário ambiente que permanentemente souberam cultivar.

Às Rosas da minha vida,
minha mãe pela orientação que em vida sempre me deu,
minha mulher pelo apoio que nunca me faltou.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

Desde finais de 2013 que as Forças Armadas portuguesas, nomeadamente o Estado-Maior-General das Forças Armadas, vêm desenvolvendo uma série de iniciativas no sentido de melhor se preparem para os novos desafios securitários que o ciberespaço vem proporcionando. Para o efeito, foi publicado o quadro normativo que determina as atribuições das Forças Armadas no âmbito da segurança do ciberespaço, tendo-se desenvolvido um conjunto de atividades conducentes à implementação de diversas estruturas e capacidades operativas no universo da defesa nacional.

Recorrendo a uma estratégia de investigação qualitativa, assente num método de raciocínio hipotético-dedutivo e seguindo um desenho de pesquisa de estudo de caso, constituiu objeto de investigação deste trabalho a *ciberdefesa*, entendida como a capacidade de executar operações no ciberespaço. Assim, pretendeu-se identificar contributos para a edificação de uma capacidade de ciberdefesa que assegure a atuação eficaz das Forças Armadas no ciberespaço, considerando, respetivamente, os impactos do ciberespaço como domínio operacional, a avaliação do estado da ciberdefesa nacional e a análise de diversos modelos de ciberdefesa já consolidados.

Como principais conclusões, constata-se que as Forças Armadas ainda não estão capazes de assumir o ciberespaço como domínio operacional e que o estado atual da ciberdefesa não configura, ainda, uma capacidade militar.

Palavras-chave

Capacidade, ciberdefesa, ciberespaço, domínio, estratégia e forças armadas.

Abstract

Since the end of 2013, the Portuguese Armed Forces, namely the Defence General Staff, have been developing a series of initiatives to better prepare for the new security challenges that have appeared in cyberspace. For this purpose, a legal framework was established that states the responsibilities of the Armed Forces in the field of cyberspace security, and steps have been taken towards the implementation of several structures and operational capacities in national defence.

Through a prominently qualitative research strategy based on a hypothetical-deductive reasoning method and following a case study research design, cyber defence, understood as the ability to perform operations in cyberspace, was the core issue of this research. Thus, the author has tried to identify contributions seeking a cyber defence capability that ensures that the Portuguese Armed Forces have the ability to carry on cyberspace operations, considering, respectively, the impacts of cyberspace as an operational domain, the evaluation of current cyber defence status and the analysis of several already matured cyber defence frameworks.

As main conclusions, the finding that the Armed Forces are not yet capable of assuming cyberspace as an operational domain and that the current state of cyber defence does not yet constitute a military capability.

Keywords

Armed forces, capability, cyber defence, cyberspace, domain and strategy.

Lista de abreviaturas, siglas e acrónimos

A2/AD	*Anti access and area denial*
AJP	*Allied joint publication*
ANPC	Autoridade Nacional de Proteção Civil
ANS	Autoridade Nacional de Segurança
AO	Ambiente operacional
AR	Assembleia da República
CCD COE	*Cooperative Cyber Defence Centre of Excellence*
CCD	Centro de Ciberdefesa
CCEM	Conselho de Chefes de Estado-Maior
CCOM	Comando Conjunto para as Operações Militares
CEDN	Conceito Estratégico de Defesa Nacional
CEM	Conceito Estratégico Militar
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CERT	*Computer emergency response team*
CIRC	*Computer incident response capability*
CISMIL	Centro de Informações e Segurança Militares
CNCS	Centro Nacional de Cibersegurança
COC	Comando das Operações no Ciberespaço
CPOG	Curso de Promoção a Oficial General
CSI	Comunicações e sistemas de informação
CSSC	Conselho Superior de Segurança do Ciberespaço
DGE	Departamento de Gestão e Ensino
DN	Defesa nacional
DOD	*Department of Defense*
EEM	Espectro eletromagnético
EMGFA	Estado-Maior-General das Forças Armadas
ENISA	*European Union Agency for Network and Information Security*
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EUA	Estados Unidos da América
FA	Forças Armadas
GE	Guerra eletrónica
GOV	Governo

H	Hipótese
IC	Infraestruturas críticas
IDN	Instituto da Defesa Nacional
INSA	*Intelligence and National Security Alliance*
IP	*Internet protocol*
ISO	*International Organization for Standardization*
ISR	*Intelligence, surveillance and reconnaissance*
ITU	*International Telecommunications Union*
IUM	Instituto Universitário Militar
JP	*Joint publication*
MA	Modelo de análise
MD	Ministério da Defesa
MDN	Ministério da Defesa Nacional
NATO	Organização do Tratado do Atlântico-Norte
NEP	Norma de execução permanente
NIS	*Network and information security*
NIST	*National Institute of Standards and Technology*
OC	Operações no ciberespaço
OE	Objetivo específico
OG	objetivo geral
OI	Operações de informação
OPC	Orientação Política para a Ciberdefesa
PDMC	Publicação de Doutrina Militar Conjunta
PECC	Plano para a Edificação da Capacidade de Ciberdefesa
PGR	Procuradoria Geral da República
PJ	Polícia Judiciária
PR	Presidência da República
QC	Questão central
QD	Questão derivada
ROK	*Republic of Korea*
RRISI	Rede de equipas de resposta a incidentes segurança informática
SCADA	*Supervisory control and data acquisition*
SIS	Serviço de Informações de Segurança

SSI	Sistema de Segurança Interna
TIC	Tecnologias de informação e comunicações
TTP	Táticas, técnicas e procedimentos
UE	União Europeia

Introdução

> *"The operational commander in 2035 will need to be as focused on cyber as on traditional environmental factors; it will be a mainstream element of joint and 'combined arms' operations"*
>
> (UKMoD, 2015).

Enquadramento e justificação do tema

Subordinado ao tema *contributos para uma estratégia nacional de ciberdefesa*, constituem elementos balizadores do presente trabalho o estudo e análise da ciberdefesa na sua dimensão prática, procurando suscitar informação que contribua para a edificação e operacionalização da capacidade de ciberdefesa nas Forças Armadas (FA).

O imparável desenvolvimento das tecnologias de informação e comunicações (TIC), suporte do conceito mediaticamente conhecido por globalização, vem potenciando uma acrescida interação e interdependência dos vários domínios da expressão humana, contribuindo inequivocamente para o bem-estar e desenvolvimento dos povos e países.

Paradoxalmente ao progresso e homogeneização social e cultural, a globalização tornou "também, possível uma difusão equivalente de ameaças e riscos em todas as dimensões, que incluem tanto a projeção das redes terroristas e de crime organizado, como a proliferação das armas de destruição massiva, a fragilização de Estados e o potencial devastador dos ataques cibernéticos" (IDN, 2013a, p. 515), acarretando *per se* uma dimensão de conflitualidade que pode fazer colapsar a estrutura tecnológica de suporte às funções vitais da sociedade, exigindo a intervenção pronta e eficaz do Estado português e, por essa via, determinar a necessidade de atuação das suas FA.

Com efeito, "o desenvolvimento tecnológico fez surgir novas ferramentas que, quando exploradas por atores mal-intencionados, podem ter efeitos não desejáveis, disruptivos e até destrutivos" (Nunes, 2015, p. 141), exigindo-se às FA a capacidade de operarem no ciberespaço, assegurando, também aqui, o cumprimento das missões que lhe estão atribuídas. Só assim poderá ser assegurada a flexibilidade necessária para ajustar, de forma proporcional e orientada ao objetivo, a resposta às múltiplas ameaças e desafios que crescentemente se vêm colocando às FA e a Portugal, corporizando, por esta via, a necessária e exigível presença militar neste novo domínio.

Objeto do estudo e sua delimitação

A imprevisibilidade e as dinâmicas associadas ao crescimento e impacto do ciberespaço nos diversos domínios da atividade humana colocam desafios à segurança e defesa, a que Portugal não é exceção. Neste contexto, o ciberespaço foi assume-se como

novo domínio operacional (Lopes, 2016, p. 9), determinando uma postura ativa das FA, mormente pelo desenvolvimento de capacidades militares que, face a um nível de risco aceitável, estejam dimensionadas e preparadas para mitigarem as consequências dos ataques cibernéticos.

Assim, estabeleceu-se como objeto de investigação a *ciberdefesa*, entendida como a capacidade das FA conduzirem operações no ciberespaço (OC), concorrendo para tal: a análise do quadro conceptual da Organização do Tratado do Atlântico Norte (NATO) e da União Europeia (UE); a caracterização da situação nacional; a análise e estudo de sistemas já implementados. Considerando a abrangência do tema e a necessidade de sistematizarmos coerentemente o trabalho, a investigação, a nível de tempo, espaço e conteúdo, foi orientada atendendo às seguintes delimitações:

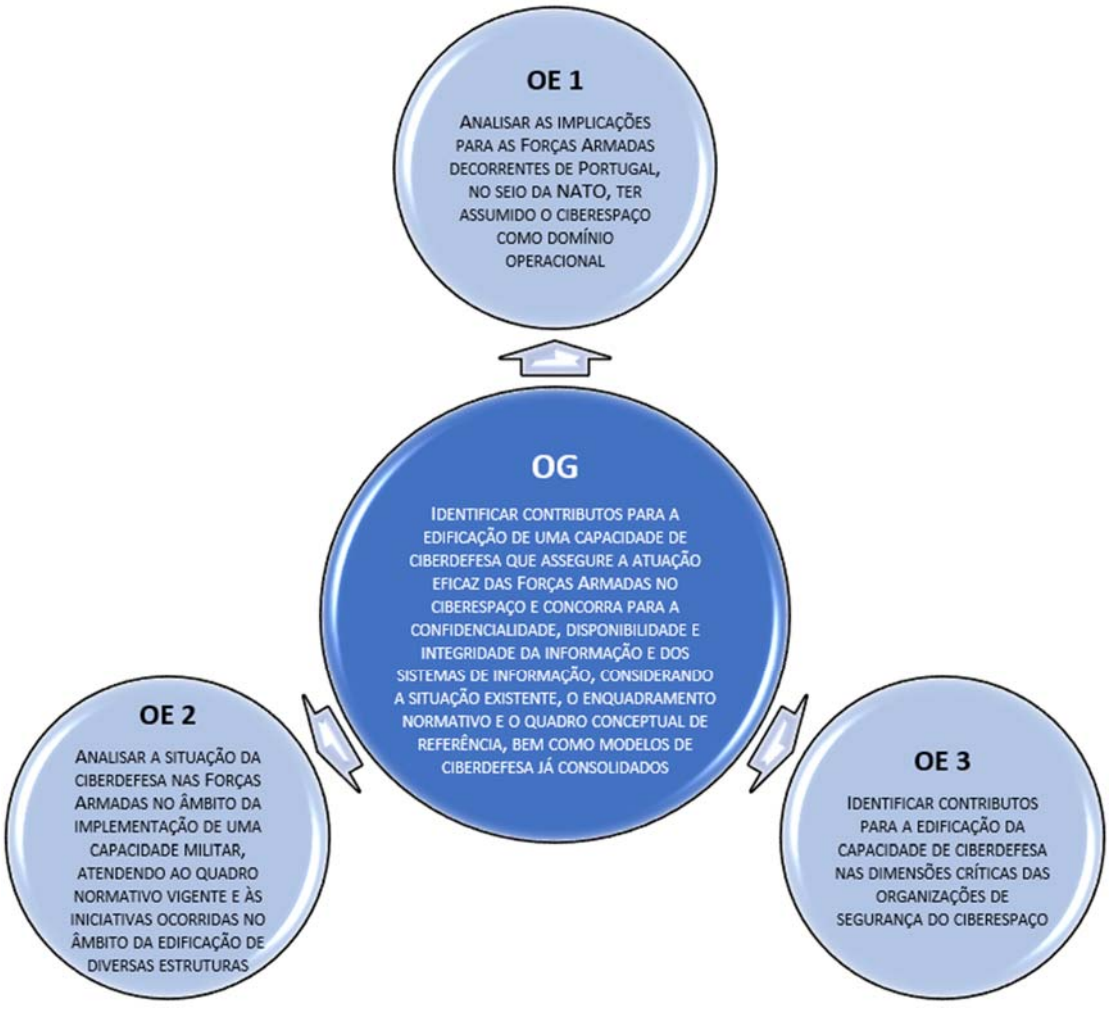
- A pesquisa e a sistematização de informação visaram identificar contributos para a edificação de uma capacidade de ciberdefesa que assegure a possibilidade das FA conduzirem OC;
- A análise conceptual teve como referência principal, quando aplicável, a doutrina militar dos Estados Unidos da América (EUA), da NATO e da UE, sem prejuízo de outras que foram pontualmente julgadas mais adequadas;
- A não abordagem da ciberdefesa ao nível tático, nomeadamente os aspetos relativos à conceção e emprego de forças;
- Os estudos de caso apresentados foram função das respostas positivas dos países - com acordos de partilha de informação de ciberdefesa - às solicitações oportunamente enviadas[1], processo que, por via da tradicional reserva que este assunto sempre merece, se revestiu da maior dificuldade;
- Análise e referências a requisitos técnicos e a ferramentas operativas, por não se enquadrarem no nível de abordagem do objeto da investigação.

[1] Em 27/10/2016, pela via diplomática sob a forma de questionário (apêndice D), com perguntas abertas à Argentina, Brasil, Chile, Colômbia e Espanha. À Coreia por interlocução direta.

Objetivos da investigação

No âmbito de uma estratégia de ciberdefesa enformadora das principais linhas orientadoras do emprego operacional e da geração de meios afins, foi definido o objetivo geral (OG) desta investigação e, enquanto elementos instrumentais para o conhecimento e para avaliação do sucesso da investigação (IUM, 2016), foram definidos os objetivos específicos (OE), conforme Tabela 1.

Tabela 1 – Objetivos de investigação



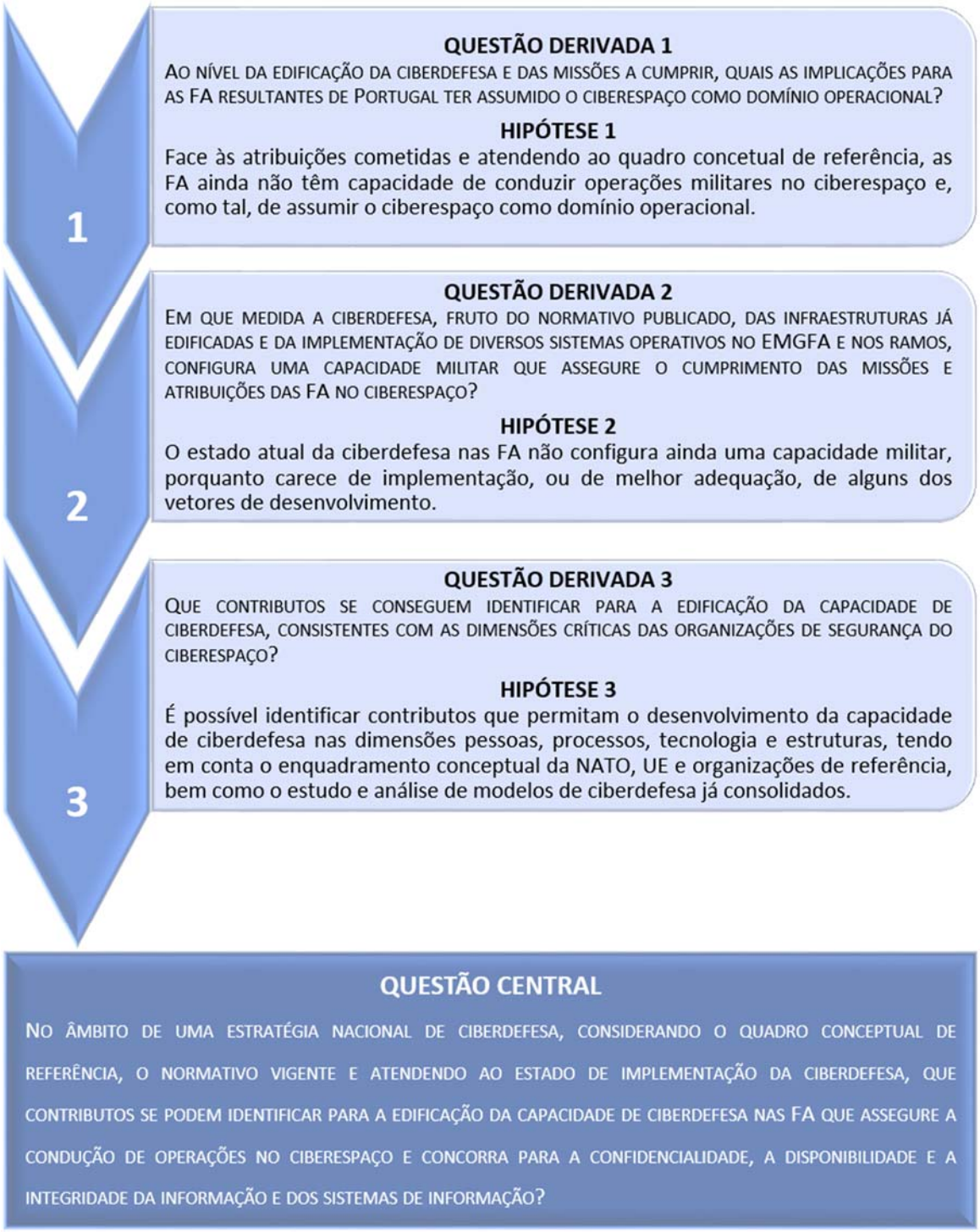
Fonte: Autor (2016)

Questões da investigação e hipóteses

Enquanto elemento fulcral da investigação (IUM, 2016, p. 51), foi formulada a questão central (QC) tendo-se enunciado as respetivas questões derivadas (QD) e respetivas

hipóteses (H), que serviram como elementos delimitadores e orientadores da investigação (Tabela 2).

Tabela 2 – Questões e hipóteses



Fonte: Autor (2016)

Metodologia da investigação

Na elaboração do presente trabalho, seguimos as orientações metodológicas em vigor no IUM (2016), tendo como referência as NEP ACA010 (IESM, 2015a) e ACA018 (IESM, 2015b), recorrendo para a referenciação bibliográfica do sistema ao estilo *Harvard-Anglia*[2], sendo o instrumento informático de apoio o *Microsoft-Word-2016*. O estudo desenvolveu-se segundo uma metodologia assente no raciocínio hipotético-dedutivo (IUM, 2016, p. 21) tendo sido adotada uma estratégia de investigação qualitativa, a partir do quadro concetual e doutrinário de países e organizações internacionais de referência, bem como de modelos já validados noutros países.

O desenho da pesquisa foi essencialmente do tipo estudo de caso, considerando o ponto de vista dos entrevistados, a análise documental das orientações e recomendações da NATO e UE e os padrões encontrados nos modelos de ciberdefesa do Brasil, Espanha e República da Coreia (ROK).

Organização do estudo.

A organização do trabalho seguiu as orientações metodológicas para a elaboração de trabalhos académicos em vigor no IUM (2016), articulando-se, suplementarmente à introdução e às conclusões, em 4 capítulos.

O primeiro capítulo inclui uma revisão crítica do estado da arte, bem como aspetos relativos à metodologia a seguir e ao modelo de análise (MA) preconizado. O segundo capítulo analisa o ciberespaço enquanto domínio operacional e as implicações que daí advêm para as FA portuguesas. O terceiro capítulo analisa a situação atual da ciberdefesa nas FA à luz da implementação de uma capacidade militar. O quarto capítulo, tendo como referência o MA, procura identificar contributos para a edificação da capacidade de ciberdefesa nacional.

A encerrar, uma síntese do trabalho, onde se procede à avaliação e discussão dos resultados obtidos, procurando dar resposta à QC, elencando-se um conjunto de contributos para o conhecimento e identificando limitações da investigação bem como eventuais linhas de pesquisa futura nesta temática.

[2] Nos casos omissos ou em que, manifestamente, se verificou a desatualização da NEP/ACA-18, privilegiou-se as regras atuais, nomeadamente a formatação, do sistema de referenciação *Harvard-Anglia* do *MS-Word-2016*.

1. Revisão da literatura e metodologia

1.1. Contexto

A ciberdefesa é uma disciplina estritamente militar, logo no âmbito das Ciências Militares, e insere-se, no que à natureza multifacetada dos contributos concerne, nas áreas de investigação (IESM, 2014, pp. 1,2) das:

– Operações Militares, subárea Guerra da Informação, porquanto é informadora da doutrina militar, nomeadamente por configurar uma capacidade militar, através da projeção de força no/através do ciberespaço;

– Técnicas e Tecnologias Militares, subárea Estudos de Componente, porquanto o ciberespaço, como domínio operacional, perspetiva a criação de mais uma componente.

Neste capítulo, pretende-se situar o objeto de investigação, relevando para o efeito: a revisão da literatura atendendo à tipologia do documento destinatário e aos conceitos principais; o modelo de análise utilizado na investigação; o percurso metodológico adotado.

1.2. Revisão da literatura

A revisão da literatura[3], bem como a investigação que lhe subjaz, orientaram-se segundo quatro linhas de ação:

– Caracterização do ciberespaço e avaliação do seu impacto nas FA enquanto domínio operacional;

– Análise dos pilares estruturantes das organizações com atribuições na segurança do ciberespaço, indistintamente de se situarem ou não na esfera militar;

– Análise da situação da ciberdefesa nacional, à luz do conceito de capacidade militar;

– Análise de modelos de ciberdefesa já implementados.

No seu prosseguimento e enquanto balizadores de toda a investigação, consideraram-se os seguintes fatores:

– O quadro normativo vigente e as atribuições cometidas às FA;

– As orientações da NATO e da UE relativas à ciberdefesa e à segurança das TIC;

– A doutrina dos EUA relativa às OC.

Como primeira reflexão, analisemos da bondade, ou não, da natureza do documento a informar – uma estratégia. No pressuposto da sua absoluta necessidade[4] como elemento catalisador de uma capacidade, interessa perceber onde se posicionará a *estratégia de*

[3] Tematicamente distribuída ao longo dos capítulos, abordando-se somente aqui os conceitos de estratégia e ciberespaço.

[4] Até por via do título previamente fixado.

ciberdefesa. Doutrinariamente, no vértice da pirâmide dos documentos concetuais e imediatamente subordinada à política, encontra-se a estratégia total, cabendo a esta "unificar, de forma coerente, todo o sistema estratégico, devendo ser entendido, não como uma simples soma ou justaposição de estratégias, mas sim, numa ótica sistémica, como a integração das várias estratégias gerais" (Couto, 1988, p. 118). Em Portugal, este documento consubstancia-se no Conceito Estratégico de Defesa Nacional (CEDN), que define os "aspetos essenciais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional" (Governo, 2013a, p. 1981).

Considerando que a cada forma de coação corresponde uma estratégia geral, estas podem subdividir-se em estratégias particulares, em função do domínio preferencial das operações que executam, resultando, no caso da estratégia (geral) militar, as estratégias (particulares) terrestre, marítima e aérea. Pela especificidade dos meios empregues e do ambiente operacional (AO) que se pretende caracterizar, é precisamente ao nível das *estratégias particulares* que se deverá situar a estratégia de ciberdefesa. Teríamos assim uma sistémica que inclui uma estratégia total, refletida no CEDN, e uma estratégia particular, correspondente à coação militar, consubstanciada no Conceito Estratégico Militar (CEM), englobando as componentes naval, terrestre e aérea. Nesta lógica e percecionando por antecipação a ciberdefesa como nova componente, reflexão a desenvolver neste trabalho, parece não fazer sentido, *per se*, a existência de uma estratégia de componente autonomizada num documento, sugerindo-se a sua inserção no CEM, em harmonia com a *praxis* corrente nas demais componentes.

Definindo planeamento estratégico como "processo contínuo de decisões sistemáticas visando o melhor conhecimento possível do futuro, por possibilitar organizar o esforço de forma sistematizada para se tomarem decisões e medir os resultados" (Drucker, 1972, cit. por Felício, 2008, p. 5), que incorpore o levantamento de cenários e a elaboração do consequente plano estratégico. Face ao OG definido, evitando a profusão de normativos e documentos conceptuais que nos afastem das competências *fazer-fazer*, pode-se inferir da maior necessidade de se elaborar um plano estratégico, ao invés de uma estratégia, que estabeleça, como corolário de todo o processo, os meios, os processos e os objetivos conducentes ao levantamento da capacidade de ciberdefesa.

Relativamente à segurança do ciberespaço nacional, apesar do acervo normativo[5] já publicado e da ativação de diversas estruturas operativas afins, esta temática ainda não

[5] Objeto de análise no capítulo 3.

mereceu, como poderia ser expectável numa lógica teoria-prática, a elaboração de um quadro conceptual de referência, tampouco a sistematização dos diversos conceitos[6], cuja verificação contribuiria para a clarificação de responsabilidades e a normalização de procedimentos nesta temática. Sem prejuízo de outros que venham a ser utilizados posteriormente, ou que venham a ser objeto de recomendação final, consideramos como conceitos informadores os apresentados no apêndice A.

No primado de que "a qualidade da estratégia nacional, num mundo globalizado, é crucial para a sobrevivência de um Estado moderno e de uma sociedade aberta" (Governo, 2013a, p. 8), o CEDN enfatiza as consequências positivas da revolução tecnológica e procedente globalização, por via de uma dinâmica de integração política, económica, social e cultural à escala mundial, alertando, no entanto, para as consequências nefastas que resultam da correspondente difusão de ameaças e riscos nas mais diversas dimensões, nomeadamente no espaço cibernético.

Pela incontornável importância de que se reveste em todo o trabalho, suscita especial atenção o conceito de ciberespaço, desde logo pela dificuldade que encerra, nomeadamente por constituir uma dimensão imaterial. Com base nos elementos comuns constantes das diversas definições do conceito, Rajnovic (2012) caraterizou o ciberespaço em função de dimensões sensoriais, de mais fácil apreensão, conforme sistematizado na Tabela 3.

Tabela 3 – Elementos do ciberespaço

ORIGEM	ELEMENTOS DO CIBERESPAÇO										
	TANGÍVEIS		INTANGÍVEIS					ÁREA DAS REDES			
	TIC	Hardware	Informação	Atividades	Aplicações e serviços	Interação humana	Virtual	Internet	Redes	Interligação	Comunicação
Oxford Dictionary							√	√			√
Alemanha	√	•	√				√	√	√	√	
Austrália	√	•	•								
Canadá	√	•	√		√	√	√		√	√	
EUA	√	√	√	√		√	√	√	√	√	√
Holanda	√	•	•								
Nova Zelândia	√	√	•						√	√	√
Reino Unido			√	√	√	√	•	√	√		√
UE		√	√				√				√
NATO Tallin Manual	√	•	√		√	√	√	√	√	√	√
ISO		√	√	√	√	√	√	√	√	√	
ITU		√	√		√	√	√	√	√	√	

√ - Ref.ª implícita • - Ref.ª explícita

Fonte: Adaptado de Rajnovic (2012)

[6] Segundo Marques (2017b), está em elaboração um glossário oficial.

Com importância decisiva no aquilatar do impacto nas operações militares, importa relevar a transversalidade e a interconexão do espaço cibernético com os outros domínios, graficamente apresentado na Figura 1, cujo conceito pode ser entendido como um "domínio global e virtual criado pela interligação de todas as redes de comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas" (NATO, 2014b).

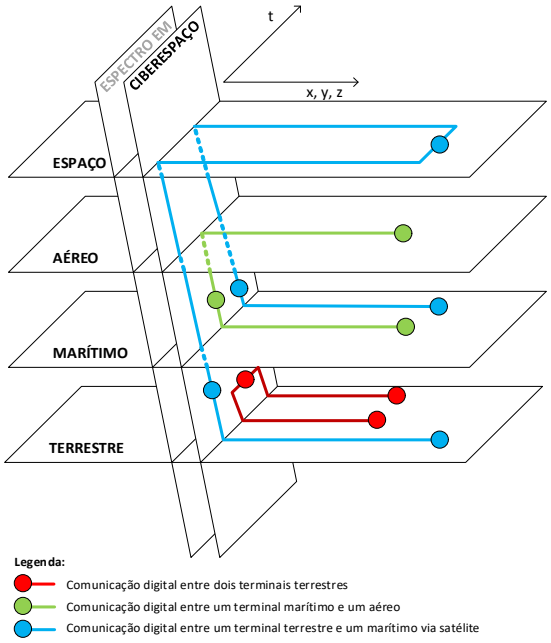


Figura 1 – Ciberespaço versus demais espaços

Fonte: Camelo, et al. (2017, p. 14)

1.3. Modelo de análise

Na sequência da revisão da literatura e da pesquisa bibliográfica definiu-se um MA, ver Tabela 4, atendendo a que:

– No domínio conceptual explicitasse os conceitos em dimensões e indicadores;

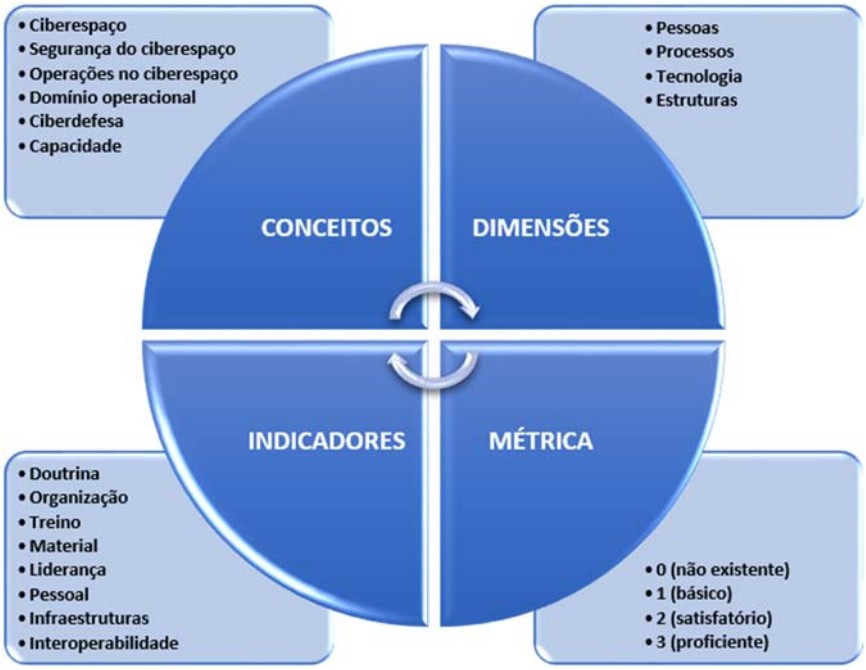
– No domínio da metodologia relacionasse os indicadores e os conceitos de modo a formular as hipóteses (IUM, 2016, p. 63);

– O conceito de capacidade militar a edificar, consequência final dos contributos a apresentar, se operacionalizasse através dos respetivos vetores de desenvolvimento (MDN, 2014a), consubstanciados como indicadores.

Baseado no modelo conceptual de referência relativo à edificação de organizações de segurança do ciberespaço (MITRE e SEI, 2014, p. 4), que define como pilares estruturantes as pessoas, os processos e a tecnologia, sistematizaram-se funcionalmente os

supramencionados vetores de desenvolvimento de capacidade, adotando-se, por via de melhor adequabilidade à organização militar e sistematização de contributos, quatro dimensões principais de análise: pessoas, processos, tecnologias e estruturas. Por último, quantificou-se o estado de implementação dos indicadores com base numa métrica da NATO (2016c, pp. 1-6), aqui adaptada a quatro níveis de maturidade.

Tabela 4 – Modelo de análise



Fonte: Autor (2016)

1.4. Percurso Metodológico

Atendendo aos OE enunciados, este trabalho utilizou uma metodologia assente no raciocínio hipotético-dedutivo (IUM, 2016, p. 21) em que se procurou dar resposta às questões derivadas, validando ou invalidando as hipóteses associadas.

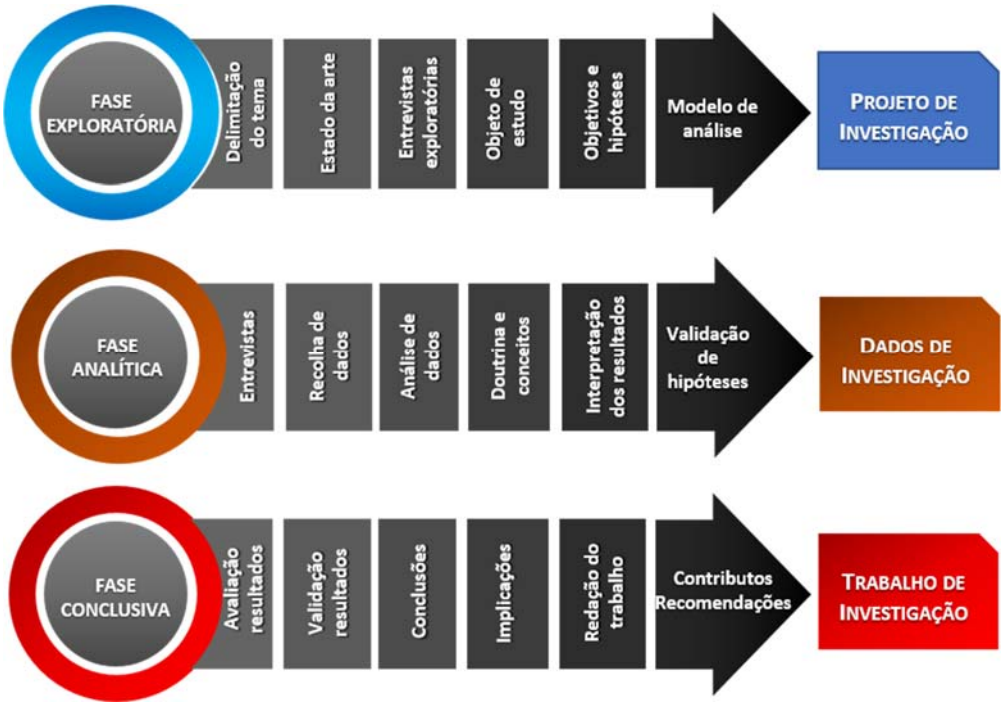
Em função da natureza do problema que se pretende estudar - a ciberdefesa - adotou-se uma estratégia de investigação qualitativa, em que se procurou elencar contributos e recomendações a incorporar no caso nacional, com base: na exploração de valores, opiniões e experiências de indivíduos referenciados na matéria (IUM, 2016, p. 29); no quadro conceptual de organizações de referência na área da cibersegurança[7]; nas orientações

[7] Carnegie Mellon, ENISA, FireEye, INSA, NIST e Saïd Business School, entre outras.

emanadas da NATO e UE; na análise de padrões obtidos a partir de modelos de ciberdefesa já validados. Consequentemente, os contributos e recomendações desenvolveram-se numa perspetiva holística e num desenho de pesquisa transversal, através do estudo e recolha de dados qualitativos de mais de um caso, com o objetivo de se detetarem padrões organizacionais num determinado lapso temporal[8]. A investigação atendeu à orientação metodológica em vigor (IUM, 2016), cuja articulação se apresenta na Tabela 5.

A escolha dos instrumentos e técnicas de recolha de dados privilegiou a análise de documentos estruturantes – ROK –, o recurso a questionários na modalidade de pergunta aberta – Brasil e Espanha[9]– e a entrevistas do tipo semiestruturada. A pesquisa bibliográfica incidiu em autores e organizações de referência na área da segurança e defesa do ciberespaço e a pesquisa documental em organizações internacionais que Portugal integra (NATO e UE), atendendo ainda à tradicional fonte de referência que é a doutrina americana.

Tabela 5 – Percurso metodológico



Fonte: Autor (2016)

[8] De 23/09/2016 a 31/03/2017.
[9] Únicos que anuíram a responder.

2. Ciberespaço como domínio operacional

2.1. Contexto

Por ocasião de uma intervenção na Assembleia da República[10], o Ministro da Defesa afirmou que "na área da ciberdefesa se esperam resultados promissores da Cimeira: a consolidação definitiva do ciberespaço como um *domínio operacional*, como um verdadeiro e novo teatro de operações – para além da terra, do mar e do ar" (Lopes, 2016, p. 9). Este compromisso, posteriormente plasmado numa resolução da NATO[11], reconhece o ciberespaço como domínio das operações, exigindo à Aliança a capacidade de se proteger e conduzir ciberoperações, similarmente ao que vem fazendo nos demais domínios (NATO, 2016d, p. 70).

À luz das referências doutrinárias habituais e dos princípios informadores das organizações internacionais a que pertencemos, este capítulo pretende caracterizar o ciberespaço enquanto dimensão operacional, abordando as implicações que daí decorrem para as FA, nomeadamente ao nível da doutrina, dos processos internos e da adequabilidade da atual estrutura de ciberdefesa.

2.2. Caracterização

Pese embora o paradoxo, enquanto dimensão imaterial, o facto é que a materialização do ciberespaço potenciou a disponibilidade e partilha de dados e informação, projetando e consolidando o conhecimento à escala global, constituindo elemento determinante do desenvolvimento e bem-estar da humanidade. Inversamente, esta "capacidade de compartilhar informações em tempo quase real, de forma anônima ou segura, é uma capacidade que é tanto um ativo como uma potencial vulnerabilidade para nós, nossos aliados e nossos adversários" (USJCS, 2014, p. ix). De facto, atentos aos dados[12] (ver Figura 2), podemos constatar uma dimensão onde simultaneamente coexistem inúmeras interações e interesses, inequivocamente potenciadores, porque inerente à condição humana, de conflitualidade.

[10] 23/06/2016.
[11] 09/07/2016.
[12] Abril de 2017.

Figura 2 – Cibernautas

Fonte: Adaptado de WeAreSocial (2017)

Neste ambiente de inigualável dinâmica evolutiva da ameaça, os estados enfrentam forças que utilizam o ciberespaço como nova dimensão da ilicitude, tirando partido das múltiplas oportunidades que este proporciona, procurando ganhar vantagem competitiva, perturbar ou interromper processos e degradar a confiança nos sistemas que suportam os serviços essenciais.

Não surpreendentemente, através de um programa robusto de ciberdefesa, a NATO (2014a) definiu que a proteção das suas redes constitui um elemento crítico para o bom cumprimento das suas missões, reconhecendo os países da Aliança, de que Portugal não constituiu exceção, o ciberespaço como novo domínio de operações, exigindo-se agora a edificação das capacidades nacionais consequentes com os princípios da defesa coletiva (NATO, 2016b, p. 1). No escopo das operações militares, a NATO (2016a, p. 5) define domínio como sendo a esfera de interesse e influência em que as atividades, funções e operações são realizadas de modo a cumprir missões e exercer o controlo sobre um adversário, a fim de se obterem os resultados desejados. A recolha e análise dos dados, em sede das doutrinas dos EUA (USJCS, 2013), da NATO (2016a, p. 2) e da bibliografia consultada, permite caracterizar o ciberespaço nos elementos que o individualizam dos outros domínios, nomeadamente:

– A dimensão imaterial enquanto produto puro do engenho humano, por contraposição à dimensão física, de natureza geográfica, dos restantes domínios;

– A elevada frequência de mudança, fruto da celeridade de processos e da cadência do desenvolvimento de tecnologias afins;

– A ubiquidade, porquanto está completamente imerso nos outros domínios, não existindo limites que configurem fronteiras;

– A possibilidade de acionamento remoto, de difícil identificação quanto à origem, proporcionando uma sensação de anonimato e, como tal, dificultar a aplicação de medidas dissuasoras compatíveis;

– O baixo custo de acesso, que facilita o empenhamento operacional e propicia o confronto assimétrico, porquanto recursos reduzidos podem originar ações hostis de elevado impacto;

– A transversalidade, pela possibilidade de afetação de todas as vertentes estrutura social;

– A natureza global, pela abrangência que alcança, permitindo a interação, ou melhor, a presença, de múltiplos atores, de diferente natureza, coexistindo neste espaço as mais diferenciadas capacidades e vontades;

– A instantaneidade, fruto da celeridade de ações que impactam a área de operações;

– A exigência da presença constante, na medida que é uma dimensão cujos processos evoluem à velocidade do código, incompatíveis com tempos de resposta dilatados no tempo e onde permanentemente a soberania tem de ser afirmada.

Percebido o ciberespaço como domínio, importa agora avaliar se pode, ou não, ser qualificado como domínio de operações, logo da guerra, recorrendo para este efeito a uma métrica da NATO (2016a), cuja validação se apresenta na Tabela 6.

Tabela 6 – Validação do ciberespaço

INDICADORES DE DOMÍNIO	VALIDAÇÃO DO CIBERESPAÇO		
	SIM	NÃO	OBSERVAÇÕES
Existirem capacidades específicas para operar.	●		*Necessidade de formação, competências e treino específicos, assim como táticas, técnicas, procedimentos e sistemas operacionais completamente distintos dos restantes domínios.*
Enquanto dimensão de operações não estar totalmente englobado por um outro domínio.	●		*Por oposição e pelas suas caraterísticas intrínsecas, o ciberespaço é o elo comum aos outros domínios.*
Permitir a presença partilhada de capacidades amigas e oponentes.	●		*Condição em que o ciberespaço é uma dimensão de referência, pelo baixo custo e facilidade de acesso, proporcionando o desencadear de conflitos assimétricos.*
Permitir exercer o controlo sobre eventuais oponentes, através da influência ou dominância.	●		*Requisito verificado, nomeadamente através do controlo parcial e localizado no tempo de determinada parte do ciberespaço, ou pela negação do acesso ao oponente, ou, ainda, em apoio das Operações de Informação, exercendo influência de modo a moldar opiniões e comportamentos.*
Ter capacidade de estabelecer sinergias com os outros domínios.	●		*O ciberespaço, na sua transversalidade, é referência pela possibilidade de apoiar ações desenvolvidas nos restantes domínios, devendo para o efeito estar integrado no planeamento geral das operações.*
Permitir desenvolver ações assimétricas através dos outros domínios.	●		*Muitas das ações no ciberespaço exigem reduzidos investimentos comparativamente às atividades ou operações nos outros domínios, em contraponto aos efeitos maximalistas que podem ser produzidos.*

Fonte: Autor (2017)

A par do desenvolvimento exponencial das tecnologias disponíveis no mercado, também os agentes promotores de atividades maliciosas vêm incrementando, com uma frequência absolutamente inacreditável, as táticas, técnicas e procedimentos (TTP) no ciberespaço, constituindo a partilha de informação uma das respostas mais eficazes à versatilidade dos ciberataques. Segundo o *Federal Bureau of Investigation* (Shaw cit. por Ackerman, 2015a), pese embora o primeiro pilar da cibersegurança residir na cooperação e partilha da informação, importa explicitar o seu real significado sob pena de poder determinar, por excesso de informação, a paralisia operacional. Efetivamente, "nesta era, já não da *Internet of Things,* mas da *Internet of Everything*, a preservação do ciberespaço de interesse nacional, numa perspetiva securitária, está desde logo alicerçada em mecanismos e processos de cooperação e partilha de *cyber intelligence*, nomeadamente a associada às ameaças identificadas e às vulnerabilidades detetadas ou exploradas, por forma a que, com oportunidade, seja extraído conhecimento acionável" (Camelo, 2016b).

2.3. Modelos de operacionalização

Caraterizado o ciberespaço nos aspetos que importam ao presente estudo, ressalta agora a necessidade de se proceder à respetiva conceptualização operacional, ou seja, modelar o ciberespaço na perspetiva de constituir um teatro de operações militares.

2.3.1. Estados Unidos da América

O JP3-12 (USJCS, 2013, pp. I-2) aborda o novo AO (ver Figura 3) estabelecendo a:

– Estratificação do ciberespaço nas camadas física[13], lógica[14] e social[15], significando esta última os aspetos cognitivos e humanos, e, como tal, o mais alto grau de abstração de um domínio operacional.

– Tipologia de OC, em ofensivas, defensivas (nas vertentes defensivas internas e resposta defensiva) e de sustentação das comunicações e sistemas de informação (CSI) da defesa.

– Categorização das atividades no ciberespaço em: defesa; informações, vigilância e reconhecimento do ciberespaço; preparação operacional do ciberespaço; ataque[16].

[13] Compreende a parte material do ciberespaço (infraestruturas de rede, sistemas e equipamentos, indexando a sua localização).
[14] Compreende as ligações entre os elementos da rede (transmissão e armazenamento de dados).
[15] Compreende as componentes pessoas física e ciberidentidades - endereços de email, de IP ou nome de utilizador (Neves, 2015, p. 16).
[16] Visando negar (degradar, interromper ou destruir) e manipular.

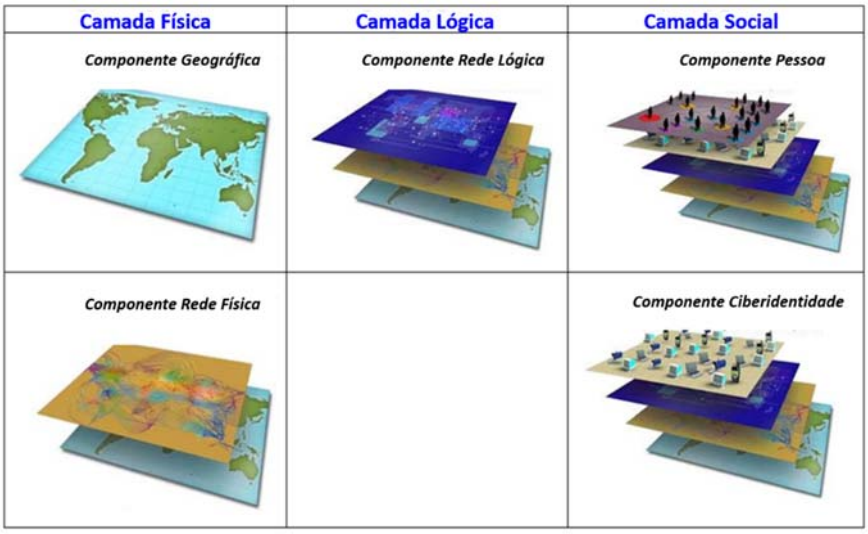


Figura 3 – Estrutura do ciberespaço (EUA)

Fonte: Adaptado de USJCS (2013, pp. I-3)

2.3.2. NATO

Com algum atraso relativamente às iniciativas de alguns países membros, também a NATO assumiu o ciberespaço como domínio operacional (2016d) tendo encetado a correspondente operacionalização, definindo:

– Uma estrutura de seis camadas (ver Figura 4):

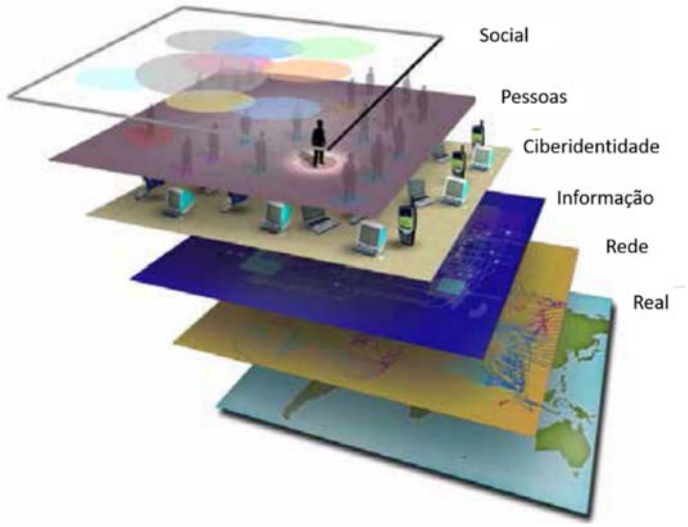


Figura 4 – Estrutura do ciberespaço (NATO)

Fonte: Adaptado da NATO (2017a, p. 18)

– Uma tipologia das operações (2017a, p. 33) em defensivas[17] e ofensivas[18].

– Uma categorização das operações quanto aos efeitos a produzir: negar, degradar, interromper e destruir (2017a, pp. 36-37).

2.3.3. União Europeia

Embora não seja uma organização puramente militar, a questão da segurança do ciberespaço da União ditou a necessidade de se elaborarem alguns princípios reguladores. Assim, o espaço cibernético é considerado como um domínio onde os adversários procuram, sob a capa do anonimato e numa lógica de não atribuição de responsabilidades, obter vantagens assimétricas em objetivos de natureza securitária, militar e, ultimamente, também de natureza política. No desempenho das missões específicas da UE e dos estados membros, o ciberespaço é entendido como um domínio igualmente crítico, devendo ser considerado como domínio operacional (UE, 2016c, p. 10). Decorre daqui um conceito de ciberdefesa orientado para o apoio às operações (UE, 2016c, p. 32), visando garantir a liberdade de ação no ciberespaço de forma a alcançar os objetivos operacionais, negar a liberdade de ação aos adversários e potenciar outras atividades operacionais. Compreende as operações em redes federadas de missão, defensivas, exploração e ofensivas.

2.4. **Implicações na doutrina militar**

Na perspetiva militar, a assunção do ciberespaço como domínio operacional tem como efeito imediato a perceção das redes CSI não apenas como plataforma de serviços, mas, sobretudo, como plataforma de operações, onde podem ser atingidos objetivos que concorram para o sucesso das operações militares. Este novo paradigma, determinante na formulação doutrinária, exige uma mudança de mentalidade, de uma perspetiva de garantia da informação para uma perspetiva de garantia da missão. A primeira revela uma postura securitária direcionada à preservação da informação e dos sistemas associados, enquanto a segunda enfatiza o impacto operacional das ações no ciberespaço. Para a NATO (2016a), no contexto do planeamento geral das suas missões, reconhecer o ciberespaço como um domínio significa desde logo implementar mecanismos de coordenação ao nível estratégico no sentido de desconflituar os efeitos nas operações, bem como incrementar ainda mais a resiliência dos sistemas de C2 e de *situational awareness*.

[17] Preservar a capacidade de usar o ciberespaço, englobando medidas ativas e passivas.
[18] Projetar força para atingir objetivos no/através do ciberespaço, englobando medidas de apoio e medidas ofensivas.

2.4.1. Operações híbridas

Enquanto fusão de diferentes capacidades e táticas num conflito, eliminando ou atenuando as fronteiras estabelecidas entre os diferentes domínios operacionais, através do emprego de métodos convencionais e não convencionais, a guerra híbrida, não sendo um fenómeno novo, encontrou na componente cibernética um instrumento de elevado potencial, em função do custo reduzido, rapidez de atuação, sensação de anonimato e crescente leque de alvos remuneradores. Sensível ao princípio de que, no âmbito da segurança dos estados, o desenvolvimento de capacidades se faz na complementaridade das vertentes interna e externa[19], a UE definiu o conceito de ameaça híbrida (ver apêndice A), tendo difundido uma diretiva (UE, 2016a, pp. 11-12) relativa à segurança das redes e da informação, visando minimizar as vulnerabilidades das infraestruturas críticas (IC) e criar uma rede, distribuída pelos países, de 28 equipas de resposta a incidentes de segurança informática e uma equipa central de resposta a incidentes de segurança informática para efeitos de uma cooperação operacional. Salienta-se que estas iniciativas estão em linha, também, com as preocupações manifestadas por Portugal, ao considerar que "hoje, o conceito de ameaça vai muito para além do que dantes associávamos ao estritamente militar, podendo ter configurações como recentemente a Rússia mostrou, num teatro de operações muito complicado como foi a Ucrânia" (Lopes, 2016).

2.4.2. Simultaneidade de efeitos e convergência

A análise da doutrina de emprego dos meios de guerra eletrónica (GE) e das ações que compreende, permite encontrar pontos em comum com as OC, não olvidando que a dimensão onde se situa a GE – o espectro eletromagnético (EM) – constitui parte integrante do ciberespaço. É natural que na ótica da sistematização doutrinária, da coordenação de procedimentos, da racionalização de recursos e da maximização dos efeitos, se suscite a necessidade de analisar conjuntamente estas duas vertentes das operações. Nesta perspetiva e evocando o princípio da simultaneidade (Simpkin, 1987, cit. por Neves, 2015), em que a tónica operacional não está na simultaneidade das ações, mas sim na simultaneidade dos efeitos, constitui referência o trabalho desenvolvido pela Rússia[20] visando uma capacidade integrada com meios de GE e de ciberguerra (Seffers, 2016, p. 48). Esta reorganização das capacidades do ciberdomínio, enquadra-se no princípio do "*near-simultaneous neutralization of all depths of the enemy's defense*" (Simpkin, 1988, p. 145), que, numa

[19] Princípio que Portugal, apesar da evidente escassez de recursos, tarda em implementar.
[20] Aproveitando a enorme experiência que, desde a guerra fria, detém no domínio da GE.

abordagem absolutamente simplista, se objetiva na negação da capacidade de reação por empenhamento (leia-se exaustão) de todos os recursos do oponente.

Esta convergência encontra-se também em estudo nos EUA, perspetivando-se a sua integração num comando único que articule e maximize ambas as capacidades que, sendo diferenciadas, utilizam o EM em larga escala (Loerch, 2016, p. 29).

2.4.3. Operações multidomínio e A2/AD

Na doutrina militar, o emprego de capacidades no ciberespaço vem revisitar a aplicação do conceito de *anti access* e *area denial* (A2/AD), sobretudo ao nível estratégico, centrado agora na exclusão do ciberespaço ao oponente, ou, no limite, na possibilidade de um estado ser desligado inteiramente do ciberespaço (Russell, 2017). De facto, o aumento da dependência dos sistemas que suportam a sociedade do conhecimento das TIC, como tal necessitando de acesso ao ciberespaço, configura uma nova vertente de aplicação do conceito A2/AD, nomeadamente a realização de operações A2/AD de nível estratégico no ciberespaço, não sendo despiciendo considerar, doravante, a exclusão do ciberespaço como ferramenta coerciva da diplomacia.

O incremento das TIC, a par dos recentes desenvolvimentos na área da robótica e da modelação, características intrínsecas à quarta revolução tecnológica (Schwab, 2016), colocam desafios securitários que exigem novas posturas das lideranças militares, especialmente nos processos relativos à condução das operações. Impõe-se salientar que o sucesso militar, nas campanhas atuais, não está mais centrado no esforço num só domínio, mas sim na utilização sincronizada das capacidades em vários domínios, desenvolvendo operações simultâneas. Não quer isto dizer, e daí a novidade, que estejamos perante o conhecido paradigma das operações conjuntas, de que, aliás, as FA detêm a necessária experiência e conhecimento, mas sim de um novo conceito centrado nas denominadas operações multidomínio. De acordo com a doutrina americana (2016, p. 2), o conceito de multidomínio compreende as operações, capacidades e soluções que empregam ferramentas específicas de um domínio para criar efeitos noutro domínio. Este conceito, apenas possível pelo surgimento do domínio imaterial[21], assenta na ideia de elevar substancialmente o nível de integração dos equipamentos e sistemas, a um patamar em que possam interoperar nos diversos domínios, apoiados em tecnologias e processos de integração e fusão de dados assistidos por inteligência artificial (Boutherin, 2017, p. 68). Conforme realçado pelo *Joint Chief of Staff* (2016), a caracterização do ciberespaço é informada pela ideia de que

[21] Leia-se ciberespaço.

atividades do elemento opositor desenvolvidas neste domínio podem afetar a execução das nossas operações em diversos domínios, pela cada vez maior interligação e dependência dos domínios tradicionais relativamente ao ciberespaço.

2.5. Situação nacional

O ciberespaço e as tecnologias que o suportam, enquanto promotoras da sociedade do conhecimento, potenciam também uma nova dimensão da conflitualidade que, no limite, pode atentar contra a segurança nacional, exigindo às FA portuguesas a capacidade de, também aqui, cumprir a defesa nacional. De acordo com Brandes (2013, p. G93), o primeiro desafio organizacional situa-se ao nível da mudança cultural, mormente das lideranças militares, preparando os diferentes escalões para entenderem que esta componente não deve ser encarada isoladamente, mas conjuntamente com as demais.

Pese embora a estrutura da ciberdefesa nacional, enquanto capacidade, ser objeto de estudo no capítulo posterior, a análise *in loco* aos órgãos que a integram, especificamente o Centro de Ciberdefesa (CCD) e os núcleos *computer incident response capability* (CIRC), permite aferir que estão organizados numa lógica securitária (*information assurance*), configurando apenas capacidades operativas na área da segurança das CSI. Também nas vertentes doutrinária e funcional, não se identificam TTP orientadas para as OC, inexistindo ao nível estratégico-operacional uma estrutura afim, tampouco ao nível tático – Marinha (Pires, 2016), Exército (Pires, 2016) e Força Aérea (Vicêncio, 2016) – existem equipas com valências ciber[22]. Para mitigar esta vulnerabilidade, Monteiro (2017, p. C1) anui na necessidade de fazer evoluir o atual CCD para uma estrutura de comando para a componente cibernética, onde devem ser desenvolvidos mecanismos para que, em situações de crise ou guerra, este órgão possa alargar a sua ação às infraestruturas estratégicas, que as define como sendo aquelas cujo não funcionamento pode afetar parte ou o todo nacional. Este comando, a implementar, deverá ter uma "natureza integradora, devendo ter uma estrutura preparada para incluir, por crescimento face a uma situação de crise e em situação de treino, posições para representantes dos principais órgãos que concorram para a segurança do ciberespaço nacional, potenciando assim a cooperação e a troca de informação que considera essencial face à natureza transversal deste domínio" (Monteiro, 2017, p. C1).

Partilhando a ideia de uma estrutura vocacionada para o comando de uma nova componente, Cunha (2017) refere a necessidade de criar, na esfera de ação do Comando Conjunto para as Operações Militares (CCOM), um "comando específico, considerando as

[22] *Cyber work force*.

capacidades cibernéticas como um sistema de armas que deverá ser utilizado nas seguintes áreas: ao nível estratégico, integrado na segurança do país; na aquisição de informações relativamente a riscos e ameaças[23]; integrado nas operações militares, junto com o CCOM, de modo a assegurar a coordenação com os ramos das FA e contribuir para o cumprimento das missões operacionais". Impõe-se elaborar um conceito de operações que estruture a tipologia de OC, defina as responsabilidades dos elementos intervenientes e articule as capacidades cibernéticas ao nível funcional e operativo.

Também na dimensão *pessoas*, a dinâmica e a complexidade do ciberespaço exigem uma adaptação contínua à envolvente operacional, colocando às FA o desafio adicional de recrutar e reter o pessoal mais qualificado, capaz de integrar os requisitos inicialmente estabelecidos e, proativamente, promover a inovação e a evolução constante, tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades.

2.6. Síntese conclusiva

A natureza global do ciberespaço determina um infindável número de interações positivas, fomentadoras da prosperidade e bem-estar, mas também de nova conflitualidade, potenciada pelas características intrínsecas desta dimensão, nomeadamente as que resultam da inexistência de fronteiras, da sensação de anonimato e da facilidade e baixo custo de acesso. De facto, as ameaças veiculadas pelo ciberespaço serão interpretadas por uma panóplia cada vez mais vasta de protagonistas, com objetivos que ultrapassam os sistemas militares, focados sobretudo nas denominadas infraestruturas críticas e nos serviços essenciais que sustentam o modelo das sociedades ditas ocidentais. Os ataques serão cada vez mais dissimulados, aumentando a incerteza relativa à sua efetiva ocorrência e dificultando a identificação da sua verdadeira origem.

Do ponte de vista militar, entender o ciberespaço somente como uma plataforma de prestação de serviços ao nível das TIC, em detrimento de o reconhecer primariamente como domínio operacional, poderá acarretar riscos à segurança nacional, que a defesa e em particular as FA portuguesas não podem descurar, evitando, também por esta via, fazer transparecer uma imagem de fraqueza operacional nos outros domínios, possibilitando ou encorajando eventuais oponentes a exercer o controlo e influência no espaço cibernético nacional.

[23] Com dependência técnica do CISMIL.

Assumir o ciberespaço como o 4º domínio[24] de operações significa, desde logo, para as FA uma mudança de abordagem da ciberdefesa, de uma perspetiva centrada na segurança da informação para uma perspetiva orientada para a execução de operações. Na ótica militar, operacionalizar o ciberespaço significa assumir relativamente a este uma postura idêntica à adotada nos outros domínios operacionais, o que equivale a considerar o ciberespaço como mais uma dimensão que concorre, com acuidade crescente, para o cumprimento da missão. Às FA portuguesas coloca-se o desafio de edificar uma capacidade de ciberdefesa credível e coerente, que assegure a condução de operações no ciberespaço, concorrendo para tal desiderato a integração desta componente em todas as fases do planeamento das operações militares.

Da análise à situação nacional, nomeadamente ao CCD, conclui-se do desajustamento para assumir o paradigma do ciberespaço enquanto domínio de operações, por via da inexistência de uma estrutura orgânica compatível que comporte os requisitos operacionais, funcionais e técnicos mínimos que habilitem as FA a operar no ciberespaço. À semelhança do que ocorre conceptualmente nos outros domínios, este desiderato só poderá ser alcançado com uma estrutura de ciberdefesa implementada aos diferentes níveis, concebida numa lógica de comando de componente (estratégico-operacional) e com valências ao nível tático (ciberequipas). Também na área dos processos, não se verificou ainda o impacto desta nova realidade, nomeadamente ao nível da integração das OC no planeamento geral das operações bem como das aludidas sinergias com as restantes áreas de atividade no EM, de que a GE constitui importante referência.

No plano doutrinário e dos consequentes processos de formação e aprendizagem, não existem referências nacionais, nem a um esquema específico de operacionalização do ciberespaço nem ao conceito multidomínio, sendo que este último se predispõe vir a ser o elemento enformador das operações no futuro próximo e cuja implementação reside nas reconhecidas potencialidades que o ciberespaço e as tecnologias associadas disponibilizam às capacidades militares, orquestrado no princípio sinérgico de que o todo – multidomínio – é maior do que a soma das partes - domínio. Esta aceção diferencia-se do tradicional conceito do *conjunto*, na medida que este representa a utilização integrada de capacidades das diferentes componentes, em contraponto ao multidomínio em que a integração se faz entre as capacidades das componentes nos diversos domínios, sem a preocupação clássica de se

[24] Exclui-se o espaço por ausência de capacidades nacionais.

predefinir antecipadamente qual, deixando esse critério a ser implementado automaticamente pelas plataformas tecnológicas de última geração.

Analisadas nas diferentes dimensões as implicações do ciberespaço como domínio operacional e avaliada a situação nacional, conclui-se que as FA ainda não estão capazes de executar operações no ciberespaço, considerando-se validada a H1, respondida a QD1 e atingido o OE1.

3. A ciberdefesa nas Forças Armadas

3.1. Contexto

O ciberespaço, no seu caráter dual de promotor de progresso e bem-estar social, mas também vetor de novos riscos e ameaças, vem suscitando, no caso nacional, a definição do quadro legal de atuação das FA que alicerce a posterior edificação das respetivas capacidades militares. Ao nível político-estratégico, considera o Instituto da Defesa Nacional (IDN) que o ciberespaço "constitui hoje um vetor estratégico privilegiado para o desenvolvimento cultural, social e económico e para a defesa dos valores das modernas sociedades da informação, requerendo por essa razão uma clara perceção do quadro das ameaças e vulnerabilidades a ele associadas" (2013b, p. 5).

No firme propósito de fazer face ao aumento e sofisticação das atividades cibernéticas hostis e atendendo às missões que incumbem às FA no quadro da soberania e garantia da liberdade de ação no ciberespaço, assume-se como essencial a implementação da capacidade de ciberdefesa. Considerando os indicadores e dimensões estabelecidos no MA, constitui objetivo deste capítulo, estudar, caracterizar e avaliar o estado de implementação da capacidade de ciberdefesa nas FA.

3.2. Quadro normativo e conceptual

A ciberdefesa, conceito de natureza exclusivamente militar, mereceu de Portugal uma abordagem político-estratégica consubstanciada, primeiro num quadro normativo, em alguns aspetos conceptual, e posteriormente na definição de uma estrutura operativa que sustentasse a operacionalização da capacidade. Procedeu-se, para o efeito, à publicação de um conjunto de documentos, apresentados cronologicamente na Figura 5, de que se ressalvam, sempre numa lógica de dimensões e indicadores do MA, os aspetos considerados essenciais.

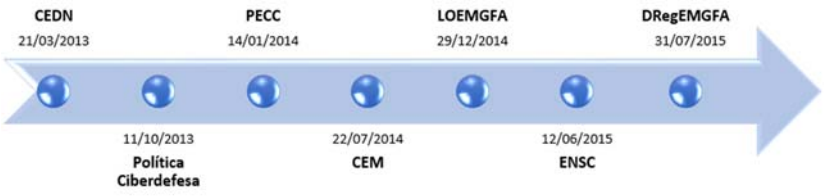


Figura 5 – Normativo da ciberdefesa

Fonte: Autor (2017)

O CEDN, documento balizador da estratégia geral, fixa a cibercriminalidade como risco e ameaça à segurança nacional "porquanto os ciberataques são uma ameaça crescente às IC, em que potenciais agressores (terroristas, criminalidade organizada, estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" (Governo, 2013a, p. 16). Consonante com o OG definido, o CEDN sublinha a necessidade de se implementar uma nova capacidade militar, considerando, como linha de ação prioritária no domínio da cibercriminalidade, entre outras, o levantamento da capacidade de ciberdefesa (Governo, 2013a, p. 34), e que as "alterações estruturais no ambiente de segurança e a natureza das ameaças à segurança nacional implicam uma capacidade de resposta diferente das FA" (Governo, 2013a, p. 36).

A Orientação Política para a Ciberdefesa (OPC) apresenta o quadro geral das ameaças e riscos do ciberespaço, constituindo-se como documento iniciador de todo o processo de edificação da capacidade de ciberdefesa, mencionando o impacto do ciberespaço na segurança e defesa nacional. Abrangendo já, diga-se até de modo inovador, a vertente da ciberdefesa orientada à missão, a OPC explicita que "o ciberespaço constitui um novo domínio operacional, onde podem vir a ser conduzidas operações militares e onde o levantamento de mecanismos de proteção e defesa obedece à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado" (MDN, 2013, p. 31977). Numa lógica de estratégia operacional, refere ainda a necessidade de dotar as FA dos mecanismos necessários para o "ambiente do moderno campo de batalha, cada mais descontínuo e multidimensional, constatando-se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações[25] em redes de computadores, juntando aos tradicionais espaços de atuação[26] também o ciberespaço" (MDN, 2013, p. 31978), ressalvando ainda que:

- As FA dependem, cada vez mais, da livre utilização do ambiente de informação e do próprio ciberespaço para conduzirem todo o espectro de operações.
- As atividades de ciberdefesa são orientadas para atender às necessidades da defesa nacional visando assegurar a utilização do espaço cibernético, impedindo ou dificultando o seu uso contra os interesses nacionais nos tradicionais espaços de atuação e também no ciberespaço.

[25] Defensivas, de exploração e ofensivas.
[26] Terra, mar e ar.

Na dimensão *estruturas*, a OPC levanta a necessidade de uma estrutura de comando e controlo da ciberdefesa nacional, alicerçada num órgão com caráter de orientação estratégica-militar das atividades de ciberdefesa e uma capacidade militar de resposta operacional a ciberataques e a incidentes informáticos. Para o efeito preconiza a constituição do CCD, na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), como "órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas" (MDN, 2013, p. 31978).

O CEM, documento que protagoniza a estratégia militar, identifica os cenários gerais de emprego das FA. O primeiro, relativo à segurança e defesa do território nacional e dos cidadãos, está dividido em sete subcenários de que se destaca, porque no âmbito dos contributos a desenvolver neste trabalho, o subcenário Ciberdefesa. O CEM tipifica o conceito de ciberdefesa como relativo a "aplicação de medidas de segurança que garantam a salvaguarda da informação e a proteção das infraestruturas de (CSI) das FA contra ciberataques, bem como o apoio, no caso de um ciberataque, à proteção e defesa das IC nacionais e do governo eletrónico do Estado" (CCEM, 2014, p. 19). Este aspeto encontra-se também vertido nas Missões das FA (MIFA), nomeadamente na M1.6-ciberdefesa (CSDN, 2014, p. 3).

No entanto, é no seguimento da Lei Orgânica (Governo, 2014d) do Estado-Maior-General das Forças Armadas (EMGFA) que se encontram os contributos principais na variável *organização*, ao especificar as competências do CCD, enfatizando que compete a este "assumir a direção e coordenação da capacidade nacional de ciberdefesa, nomeadamente conduzir operações militares no ciberespaço" (Governo, 2015b, p. 5287).

Por último, em 2015, foi publicada a Estratégia Nacional de Segurança do Ciberespaço (ENSC) que, na área da ciberdefesa, informa os elementos passíveis de serem incorporados na dimensão *processos*, referindo a necessidade de "aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das IC e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (Governo, 2015f, p. 3738). A ENSC, cuja execução[27] se apresenta na Tabela 7, articula-se em seis eixos de intervenção, estabelecendo, no âmbito da estrutura de segurança do ciberespaço[28], a

[27] Referida a 13/01/2017.
[28] Eixo 1.

necessidade de "implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional" (Governo, 2015f, p. 3740). Apesar da louvável clareza conceptual de significar ciberdefesa com OC, deteta-se uma omissão importante, que se julga dever ser corrigida na próxima revisão, por ausência de atribuições às FA no Eixo 3 (Proteção do ciberespaço e das infraestruturas).

Tabela 7 – Execução da ENSC

EIXOS DE INTERVENÇÃO	MEDIDAS				
	Total	Executadas	Em execução	Não iniciadas	Estado desconhecido
1. Estrutura de Segurança do Ciberespaço	27	0	24	0	3
2. Combate ao Cibercrime	2	1	0	0	1
3. Proteção do ciberespaço e das infra-estruturas	17	1	15	0	1
4. Educação, sensibilização e prevenção	10	2	2	3	3
5. Investigação e desenvolvimento	6	0	0	0	6
6. Cooperação	9	3	5	0	1
	71	7%	46%	3%	15%

Fonte: CNCS (2017)

A análise dos diplomas mencionados permite inferir da progressiva evolução do conceito de ciberdefesa, procurando acompanhar a mudança de paradigma, conforme referido no capítulo anterior. Paradoxalmente, é precisamente a estratégia militar (CEM) que revela ser o documento menos adequado ao paradigma, por remeter a ciberdefesa para um conceito já ultrapassado, que não reflete o ciberespaço como domínio de operações.

Por último e reiterando o já referido no capítulo primeiro, não é despiciendo refletir sobre a necessidade ou não de se elaborar uma estratégia a montante, como elemento catalisador para a implementação e operacionalização da ciberdefesa. De facto e no caso português, o edifício conceptual, no que às relações entre os documentos estruturantes e as capacidades operacionalizadas concerne, assenta numa estratégia nacional (CEDN) e em estratégias particulares que, no caso em apreço, se consubstanciam no CEM (estratégia militar), não existindo a vocação para se elaborarem estratégias específicas ao nível das componentes militares. Atentos a que o planeamento estratégico se refere ao processo de

desenvolver e implementar planos para alcançar metas e objetivos (Felício, 2008), emana a ideia de que, para a edificação da capacidade, concorre, sobretudo, a elaboração de um plano estratégico assertivo que inclua a finalidade, os objetivos a atingir e as consequentes linhas de ação estratégica.

3.3. Análise

A avaliação da *capacidade de ciberdefesa*, objeto deste capítulo, pressupõe o entendimento dos conceitos subjacentes de forma a que, objetivamente e com base no MA, se proceda à respetiva tipificação. Dos elementos apurados durante a investigação, constata-se que o conceito de ciberdefesa não se encontra definido, subsistindo apenas uma proposta do IDN (2013b, p. 11) que, face à operacionalização do ciberespaço, se revela desajustado (ver apêndice A). Por via do enviesamento ditado pela natureza iminentemente defensiva e multinacional da Aliança, deve-se também evitar a via facilitista de ancorar a definição nacional de ciberdefesa no conceito da NATO (ver apêndice A), sob pena de, fazendo-o, se operacionalizar uma capacidade inconsequente com os objetivos e atribuições superiormente fixados. É, no entanto, justo referir que a definição do conceito de ciberdefesa, sendo importante, não constitui premissa absolutamente limitadora da implementação desta capacidade militar, porquanto, por via do normativo publicado (Governo, 2015b, p. 5287), se encontram já fixadas, com detalhe considerável, as atribuições da ciberdefesa, nomeadamente do seu órgão de cúpula.

Porque essencial para a análise subsequente, enuncia-se agora o conceito de *capacidade militar*, como "o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir" (MDN, 2014a, p. 23657), devendo a sua parametrização ocorrer por via dos vetores específicos de desenvolvimento de capacidade, aqui materializados em indicadores do MA.

A estrutura[29] de ciberdefesa implementada nas FA tem como elemento informador o Plano para a Edificação da Capacidade de Ciberdefesa (PECC) que, entre diversos aspetos (EMGFA, 2014, pp. 12-13), define:

– As capacidades, englobando: deteção e resposta a ciberincidentes; monitorização permanente das redes; ferramentas de *intelligence situational awareness*; módulos/equipas

[29] Em função do conceito anteriormente definido, reserva-se o emprego do termo capacidade para o final do capítulo por via do apuramento ou não se estamos em presença de uma capacidade militar.

de ciberdefesa; mecanismos de garantia da continuidade de serviços; análise forense e mecanismos de coordenação nacional e internacional.

– A estrutura, composta pelo CCD e quatro CIRC [30].

Na dimensão *organização*, a análise à estrutura de ciberdefesa, nomeadamente dos seus os órgãos constituintes, permite constatar que estes, por via do estipulado no PECC, têm apenas especificado o efetivo em pessoal, omitindo os aspetos relativos à articulação interna, de natureza departamental, não abordando eventuais processos funcionais.

No que ao CCD respeita, o plano menciona a sua articulação em duas subestruturas[31] – não refletidas em sede da orgânica nem do serviço diário – afigurando-se necessário adequar a estrutura da ciberdefesa ao quadro de competências legais vigentes desde 2015 (Governo, p. 5287), por inadequabilidade dos órgãos existentes. Esta disfuncionalidade, nos indicadores *organização* e *pessoal*, que impossibilita as FA de assumirem o ciberespaço como domínio operacional, é também partilhada ao mais alto nível da hierarquia militar. De acordo com o Monteiro (2017) e Cunha (2017), urge fazer evoluir o CCD para uma estrutura tipo comando de componente, com dimensão adequada às necessidades e que seja capaz de lidar com o paradigma do ciberespaço ser domínio das operações militares. Relativamente à nova estrutura a erigir refere, ainda, a necessidade de "serem desenvolvidos mecanismos de ação e coordenação para que, em situação de crise ou guerra, possa alargar a sua ação às infraestruturas estratégicas, sendo estas definidas como aquelas cujo deficiente funcionamento pode afetar parte ou o todo Nacional" (Monteiro, 2017).

Em linha com a análise efetuada, as opiniões confirmam a perceção de que o indicador *organização* está insuficientemente abordado no PECC, devendo a avaliação das estruturas existentes, ou a implementação de novas, ter em consideração o conceito âmago deste ensaio, ou seja, fazer refletir nas FA a capacidade de conduzir OC. Por similaridade aos demais domínios e nomeadamente às capacidades das componentes respetivas, as OC podem ser definidas pelo emprego de cibercapacidades para alcançar objetivos no, ou através do[32], ciberespaço. Para tal, necessita-se, nos indicadores *doutrina* e *processos*, criar mecanismos e rotinas que integrem as OC no planeamento geral das operações militares, *per se,* ou constituindo elemento multiplicador do potencial de combate. Esta finalidade requer

[30] EMGFA, Marinha, Exército e Força Aérea, visando proteger a integridade, confidencialidade e disponibilidades das CSI à sua responsabilidade.
[31] Repartição de Coordenação e Repartição de Operações em Redes de Computadores.
[32] Noutros domínios.

também novos desempenhos, só alcançados através de um plano de formação orientado, preocupação que também não é abordada no PECC.

Por outro lado, a novidade do assunto e a ausência de processos instituídos, aliada às exigentes competências a adquirir, determinam, ao nível das *pessoas*, um novo paradigma da formação base e tempo de permanência em funções dos denominados *cyber warriors*, suscitando intervenção imediata, especialmente ao nível dos ramos, únicos responsáveis pela incorporação, formação de base e gestão de carreiras.

A informação pesquisada, as opiniões auscultadas e a experiência profissional do autor são unânimes em considerar que muitos dos cargos de operadores no ciberespaço podem ser providos por pessoal civil (Pires, 2016 , Monteiro e Cunha, 2017), concentrando o pessoal militar maioritariamente nas atividades de direção, de planeamento e de operação ao nível tático.

No indicador *doutrina*, releva-se a ausência de qualquer referência teórica ou prática relativa à definição de um espectro de operações que melhor balize as áreas da organização, treino, material e interoperabilidade. Na prossecução da segurança do ciberespaço nacional, conforme o normativo publicado, as missões das FA são determinadas pelo balanceamento dos fatores *impacto* e *risco social* associado, materializados em duas vertentes: no escopo da cibersegurança setorial da defesa nacional, através de uma colaboração ativa com as restantes órgãos, forças e serviços de segurança; no domínio clássico do poder militar, pressupondo ou não o uso da força, quando as ameaças apresentem um efeito disruptivo que possa fazer perigar a segurança e a soberania nacionais. Na esfera da cibersegurança, entendida como proteção dos sistemas CSI no âmbito da defesa nacional (DN), constata-se a realização de um trabalho relevante ao nível das FA, que se encontra em adiantado grau de execução por via da implementação de ferramentas operativas num cada vez maior número de órgãos da DN.

Para melhor perceção das diferentes áreas de responsabilidade e das relações de cooperação e partilha já desenvolvidas na esfera da segurança do ciberespaço, apresenta-se a Figura 6, onde merecem especial atenção os processos já estabelecidos com a NATO[33] e o Centro Nacional de Cibersegurança (CNCS)[34].

[33] Memorando de entendimento firmado em 2016.
[34] Partilha de *cyber intel*.

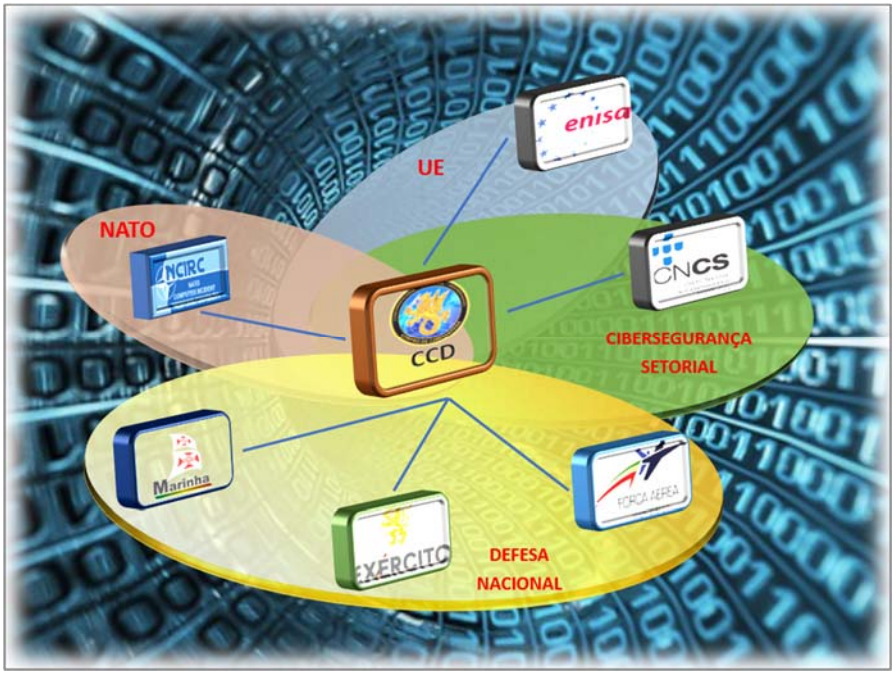


Figura 6 – CCD e a segurança do ciberespaço

Fonte: Autor (2017)

No patamar da segurança do espaço cibernético nacional, cujos contornos estão estabelecidos na ENSC, pôde-se apurar significativos avanços na implementação de estruturas nacionais, carecendo ainda de mecanismos efetivos de partilha de ciberinformação, de que é exceção a profícua relação existente entre o CCD e o CNCS. De acordo com Marques (2017a), no sentido de coordenar e articular toda a ação dos principais interlocutores da cibersegurança, está em fase de aprovação a criação de um Conselho Superior de Segurança do Ciberespaço (CSSC), conforme Figura 7.

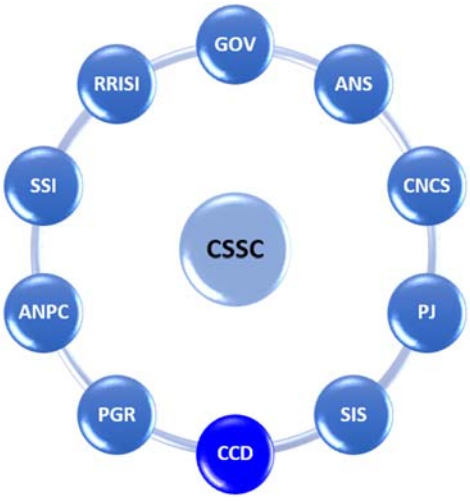


Figura 7 – CSSC

Fonte: Autor (2017)

No tocante aos *processos* organizacionais, fator importante para avaliação de uma capacidade militar, foram também identificadas lacunas, se não mesmo ausências completas, na estrutura de ciberdefesa, sublinhando Monteiro (2017) que o "maior impacto é o ainda desconhecimento dos decisores nos diversos patamares (político, estratégico e operacional) dos riscos e ameaças que se apresentam no ciberespaço e para as responsabilidades que as FA têm nesta área que considera crítica". Por via da caracterização efetuada deste novo teatro de operações, urge adaptar o *modus operandi* da tomada da decisão operacional, sob pena de, não o fazendo, estarem as FA condenadas a uma situação de não perceção da ameaça, quiçá já perpetrada, considerando "absolutamente necessário a agilização do processo da tomada da decisão que poderá passar pela criação de regras de empenhamento para as ações mais preditivas que exijam uma resposta das FA ano ciberespaço" (Cunha, 2017). Considera também o CEMGFA ser importante adaptar as *lideranças* ao novo AO sugerindo que "a agilização do processo da tomada da decisão poderá passar pela criação de um quadro de referência orientado para a sistematização dos procedimentos de ação e reação a eventos que venham ocorrer" (Monteiro, 2017).

Em função do MA adotado, julgou-se relevante para a investigação, nomeadamente para o OE2, aquilatar da perceção individual de entidades[35] (ver apêndice B) relativamente à avaliação da implementação da capacidade de ciberdefesa, cujos resultados se espelham na Tabela 8.

Tabela 8 – Avaliação da ciberdefesa

INDICADORES	MATURIDADE												
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	Média
Doutrina	0	1	1	2	2	1	1	1	1	0	1	1	1
Organização	1	1	1	1	1	1	1	2	2	1	0	1	1
Treino	1	2	1	1	2	2	2	2	2	1	1	1	2
Material	2	2	2	2	2	1	2	2	2	1	1	2	2
Liderança	0	1	0	1	1	1	1	2	1	1	1	1	1
Pessoal	0	1	1	1	1	1	0	1	1	1	0	1	1
Infraestruturas	2	2	2	2	2	1	1	2	2	1	1	2	2
Interoperabilidade	1	1	2	2	1	2	2	2	2	1	1	1	2
	Nível médio = **1**												

Métrica: 0 (não existente); 1 (básico); 2 (satisfatório) e 3 (proficiente)
E (entidade)

Fonte: Autor (2017)

[35] Com responsabilidades nas áreas de comando, direção, operação e técnica.

Realça-se, no entanto, que esta avaliação versa somente o conceito de ciberdefesa que se pretende ultrapassar, ou seja aquele orientado para a cibersegurança, não englobando o conceito orientado para as operações.

A avaliação da capacidade de ciberdefesa nas FA, entendida nas competências já institucionalizadas (Governo, 2015f, p. 3740), e cuja verificação invalidaria a H1, remeteria para um nível de implementação residual, porquanto há ainda muito por fazer nas dimensões pessoas, processos, tecnologia e estruturas. De modo a habilitar as FA a desempenharem eficazmente todo o espectro de missões no ciberespaço, face às limitações existentes, mas também atendendo ao enorme esforço que as FA vêm efetuando desde 2015, "há a necessidade de conceber um plano de implementação desta capacidade militar faseado no tempo, devendo, atendendo ao processo de planeamento das FA, ser incluído na próxima revisão da Lei de Programação Militar e da estrutura de forças, em 2018" (Monteiro, 2017).

A análise do relevante trabalho já realizado pelas FA confirma que todas as atividades se centraram na esfera da ciberdefesa enquanto promotora da segurança da informação, traduzida na edificação de uma estrutura central tipo *computer emergency response team* (CERT)[36] conectada a três CIRC nos ramos, aguardando-se a ativação de um quarto CIRC na esfera do EMGFA.

O estudo do caso nacional, ademais corroborado pelas opiniões recolhidas, coloca a tónica na necessidade de fazer evoluir o CCD para uma *organização* que, incorporando as tradicionais operações de segurança das CSI, integre também a vertente orientada para as operações, assumindo uma estrutura de comando de componente, alinhando assim Portugal com os mais de 50 países que, por evolução dos seus CERTs, militarizaram o ciberespaço assumindo-o como domínio de operações (Young-ju, 2016, p. 24). Restará, e não será tarefa simples, conceber um plano de geração de uma capacidade que, num todo coerente, articule "doutrina, procedimentos, táticas e técnicas afins que permitam sincronizar as OC com os outros domínios" (Seffers, 2017, p. 34).

Da investigação resulta ainda, face à perceção das entidades consultadas (ver Tabela 9), de que no conceito mais lato, a capacidade de ciberdefesa deve integrar prioritariamente as áreas do emprego da força, conhecimento situacional e proteção e sobrevivência.

[36] O CCD.

Tabela 9 – Ciberdefesa e áreas de capacidades

ÁREAS DE CAPACIDADE	VALORAÇÃO												
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	Total
Comando e Controlo		2	1	3	1	1		3	1		1		**13**
Emprego da Força	2		2	2		3	3			1	3	3	**19**
Proteção e Sobrevivência	1	3			3		2	2	3	3		2	**19**
Mobilidade e Projeção					2								2
Conhecimento Situacional	3	1	3	1		2	1	1	2	2	2	1	**19**
Sustentação													0
Autoridade, Responsabilidade, Apoio e Cooperação													0

Métrica: escolha de 3 áreas; valoração de 1 (mínimo) a 3 (máximo); priorização (maior valoração)

Fonte: Autor (2017)

Nos *processos*, deverá ser equacionada a articulação do nível estratégico-operacional com o nível tático, intrínseco aos ramos, e atender ainda às responsabilidades das FA nos estados de crise e guerra, considerando a necessidade de atuar num ciberespaço segmentado em três setores – público, privado e da DN – de modo a definir responsabilidades e estabelecer procedimentos de reação, nomeadamente os que se referem à prevenção, mitigação, resposta, proteção e recuperação de ciberataques.

3.4. Síntese conclusiva

A sofisticação e o aumento exponencial das atividades cibernéticas hostis reforçam a necessidade de atribuir especial prioridade à prevenção e contenção dos efeitos dos ataques que podem fazer perigar a segurança e o regular funcionamento das instituições, com especial destaque para as responsabilidades que nesta área estão cometidas às FA. Metodologicamente, o processo de implementação de uma estrutura securitária para o ciberespaço, nas competências requeridas às FA, deverá ocorrer em duas fases complementares:

– A primeira, no âmbito da garantia da informação, destinada à implementação de uma estrutura de ciberdefesa que permita prevenir, retardar e mitigar os efeitos de ações hostis no ciberespaço, através da implementação de capacidades operativas na área da cibersegurança;

– A segunda, no âmbito da garantia da missão, vocacionada para as OC, procurando integrá-las com as tradicionais operações militares, visando alcançar objetivos no ciberespaço ou constituindo-se como multiplicador do potencial de combate da força armada.

Desde 2014 que, ao nível da defesa nacional e com base no PECC, as FA[37], vêm desenvolvendo um extraordinário esforço no sentido de implementarem uma estrutura de ciberdefesa, conforme a supramencionada primeira fase, tendo-se atingido a sua capacidade operacional no final de 2016. Dos dados recolhidos e da análise efetuada, em sede das dimensões e indicadores do MA, e a bem do rigor conceptual que sempre assiste à arte e ciência militares, o PECC não preconiza a edificação de uma capacidade militar, pois não encerra elementos específicos dos vetores de desenvolvimento, tendo, contudo, o inegável mérito de ter constituído o catalisador de uma arquitetura de ciberdefesa orientada para a segurança no ciberespaço. Apesar disso, foi possível concluir que a estrutura existente, CCD e os CIRC, não assegura, conforme a legislação já determina e posteriormente reforçado por Portugal no seio da NATO, uma capacidade militar orientada para a condução de OC[38].

Numa nova etapa, impõe-se como necessário conceber um plano para a edificação da *capacidade de ciberdefesa* que, nos pressupostos operacionais apresentados, garanta o cumprimento das missões atribuídas às FA, nomeadamente aquelas que decorrem do ciberespaço ter sido considerado domínio operacional, desígnio ademais bem expresso pelas entidades consultadas, que privilegiam a ciberdefesa como capacidade prioritariamente orientada para o emprego da força e para o conhecimento situacional.

Como prioridade, nos indicadores organização, pessoas e liderança, releva-se a necessidade de: reajustar a estrutura respetivamente no nível estratégico-operacional, na lógica de um comando por domínio de operações e no nível tático, com a criação de equipas orientadas especificamente para as necessidades operacionais dos ramos; implementar uma política de pessoal orientada para as novas necessidades, a iniciar no imediato, face ao tempo prolongado que levará a surtir efeitos; desenvolver um programa de sensibilização das lideranças militares, suscitando a necessidade de integrar as CO no planeamento das operações militares.

Finalmente, e ao nível dos documentos que enquadram a ciberdefesa, reitera-se a desadequação do CEM, bem como a não necessidade de elaborar uma estratégia específica

[37] DIRCSI/EMGFA
[38] Conceito a abordar posteriormente como contributo para o conhecimento

para a ciberdefesa, pois a coerência do modelo nacional preconiza a integração das estratégias das componentes[39] num documento singular[40], bastando para o efeito proceder à sua revisão, integrando as linhas de ação estratégicas balizadoras da atuação das FA no ciberespaço.

Analisada a situação da ciberdefesa nas FA no âmbito da implementação de uma capacidade militar, atendendo ao quadro normativo vigente e às iniciativas ocorridas no âmbito da edificação de diversas estruturas, conclui-se que o estado atual da ciberdefesa não configura ainda uma capacidade militar, porquanto carece de implementação, ou de melhor adequação, alguns dos vetores de desenvolvimento. Considera-se validada a H2, respondida a QD2 e, consequentemente, atingido o OE2.

[39] Naval, terrestre e aérea.
[40] CEM.

4. Contributos para a capacidade de ciberdefesa

4.1. Contexto

Historicamente, a mutação do AO, bastas vezes suscitada pela evolução tecnológica, implica a correspondente adequação da organização militar e o desenvolvimento de capacidades específicas para fazerem face aos novos desafios. No documento *Future Operating Environment 2035* (UKMoD, 2015), o Reino Unido carateriza o AO até 2035, considerando o ciberespaço como um dos seis elementos principais[41], referindo a sua interação e afetação com os restantes domínios operacionais, salientando que todo o uso do ciberespaço que afete as IC nacionais deve ter uma resposta militar compatível. Constituindo as FA a *ultima ratio* na garantia da segurança do ciberespaço nacional, considera-se indispensável o estabelecimento de um planeamento estratégico que incorpore o ciberespaço como dimensão da afirmação da soberania nacional, definindo os "meios e os processos capazes de o atingir através de um conceito da ação estratégica" (Couto, 1988, p. 178). À luz do MA e atendendo às vulnerabilidades identificadas da estrutura nacional, este capítulo pretende elencar contributos, considerando sistemas de ciberdefesa de países e de organizações internacionais[42], bem como informação de fontes de referência.

4.2. Análise por estudos de caso

4.2.1. NATO

A NATO vem tratando com acuidade a temática da ciberdefesa (ver Figura 8), assumindo, recentemente, a dicotomia ambiente informacional[43] *versus* domínio operacional.

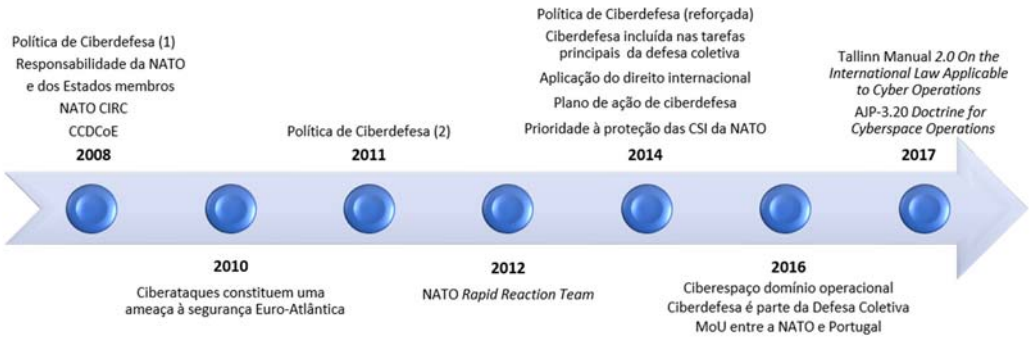


Figura 8 – Cronologia da ciberdefesa (NATO)

Fonte: Autor (2017)

[41] Atores, instituições, identidade e cultura, tecnologia e ambiente eletromagnético.
[42] Função dos compromissos internacionais.
[43] Informação, pessoas, organizações e sistemas que processam a informação.

Como ideia de partida, a NATO considera o ciberespaço como fator essencial ao bom desempenho das suas estruturas e capacidades militares, na justa medida em que estas, para operarem, têm de confiar em equipamentos, sensores, sistemas de armas e sistemas C2, cuja *performance* se baseia em múltiplas interações no ciberespaço. A eficiência destes sistemas depende da disponibilidade, integridade e confidencialidade das CSI, bem como dos valores da autenticação e do não repúdio, requisitos a observar tanto em tempo de paz como em situações de crise ou de conflito (NATO, 2017a). No ambiente internacional, onde necessariamente se consubstancia a sua esfera de interesse, a NATO reconhece a dificuldade de estabelecer critérios de comportamento, por via da inexistência de normas internacionais que regulamentem a utilização do ciberespaço. Ao nível da comunicação estratégica, a NATO vem sublinhando a utilidade do novo manual de Tallinn, que, não tendo força de lei, pode constituir um embrião de um futuro acordo internacional, que regule as responsabilidades e assim possa contribuir para a diminuição do espaço de conflitualidade cibernética.

Na vertente estritamente militar, a Aliança (2016b) considera o ciberespaço como facilitador do cumprimento das suas missões, nomeadamente por:

– Permitir atingir efeitos operacionais conjuntos de forma mais sincronizada;

– Facilitar o controlo no ciberespaço dentro da área operacional conjunta, maximizando os efeitos de defesa coletiva através da promoção da liberdade de ação e agilização do processo da tomada da decisão;

– Contribuir para divulgação de uma mensagem estratégica, reafirmando a determinação e a permanente capacidade de adaptação da postura defensiva ao cenário evolutivo da ameaça.

Refere também que o recente reconhecimento do ciberespaço como domínio operacional implica uma mudança de mentalidade e postura, diga-se também ainda não atingida em Portugal, de uma perspetiva da ciberdefesa centrada na garantia da informação para uma perspetiva orientada para a garantia da missão. Trata-se da transição do foco principal da ciberdefesa, da esfera da segurança das CSI para a esfera das operações (NATO, 2017a, p. 12), com impacto nos indicadores, conforme se apresenta na Tabela 10.

Tabela 10 – Contributos (NATO)

INDICADORES	CONTRIBUTOS
Doutrina	• Ciberespaço como fator essencial para o cumprimento da missão. • Ciberespaço como dimensão não regulada e como tal a necessitar de um acordo internacional que padronize os processos e interações de modo a responsabilizar os diversos intervenientes. • Ciberespaço como elemento de maximização da defesa coletiva. • **Conceito de ciberdefesa**: "Os meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações, da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas" (NATO, 2014b). • Conceito de *Cyber Key Terrain* (CKT) compreende: *hardware*, *software*, redes, pessoal e infraestruturas. • Tipologia de operações: ofensivas (preservar a capacidade) e defensivas (projetar força). • Capacidades no ciberespaço de natureza defensiva. • Princípios das operações no ciberespaço: segurança e surpresa (NATO, 2017a, p. 31).
Organização	• NATO CIRC com responsabilidades na área da cibersegurança. • Criação de **equipas ciber** orientadas para as operações (escalão tático). • Rearticulação das **células J6** dos estados-maiores. • Ciberoperações, ao nível dos *processos em* função de apoio CIMIC (NATO, 2017a, p. 27): Manobra (obter vantagem sobre o oponente) Fogo (arma/computador; gatilho/(tecla *enter*; projétil/código); Comando e controlo; Informações; Informação; Sustentabilidade; Proteção da força.. • **Gestão do risco** no ciberespaço: aceitar; evitar; transferir; mitigar (NATO, 2017a, p. 52).. • Ao nível dos processos: as operações no ciberespaço desempenham um papel relevante no processo de *targeting*.
Treino	• Incorporação da ciberdefesa no treino operacional.
Material	• Maior exposição ao risco dos países e organizações mais evoluídos tecnologicamente. • Gestão do risco na cadeia de aquisição e reabastecimento de TIC. • Aplicação do princípio de *security by design*. • Disponibilidade de energia como recurso vital para o ciberespaço.
Liderança	• Postura dinâmica no sentido de sensibilizar para a necessidade de integrar as operações no ciberespaço no planeamento operacional. • Flexibilização do processo de decisão.
Pessoal	• O **indivíduo** e a sua capacidade intelectual como recurso essencial.
Infraestruturas	• Mudança de tipologia dos alvos: das redes e sistemas de informação para os sistemas de controlo das infraestruturas críticas (destruição, degradação e interrupção).
Interoperabilidade	• ----------

Fonte: Autor (2017)

No campo doutrinário e visando evitar eventuais sobreposições e desconflituar efeitos, assinala-se a preocupação da NATO (2016a) em clarificar as esferas de intervenção das OC e das operações de informação (OI), ao afirmar que estas últimas integram o emprego de diversas capacidades operativas em todos os domínios com o objetivo último de influenciar o processo de tomada da decisão dos adversários, por contraponto às OC que maximizam os nossos esforços para influenciar os adversários, desenvolvendo ações para atingir objetivos no/através do ciberespaço.

Ao nível de *organização* e *pessoas*, o impacto verifica-se essencialmente na necessidade de se constituírem ciberequipas orientadas às operações, de reorganizar as células J6 dos estados-maiores, bem como reconhecer a necessidade de se ministrarem novas competências ao pessoal em funções.

No quadro das ameaças que a NATO enfrenta no ciberespaço - partilhadas também pelos estados membros - coloca-se a necessidade de uma nova abordagem à gestão do risco no âmbito da segurança das CSI, nomeadamente pela incorporação de um modelo adaptativo (NATO, 2015a) cujos *processos*, assentes na correspondência das TTP em função da tipologia de atores hostis, se encontram sistematizados na Tabela 11.

Tabela 11 – TTP e vetores de ataque (NATO)

THREAT ACTORS		OPPONENT CAPABILITY	TACTICS, TECHNIQUES and PROCEDURES												
			CNO Attacks	CNO Exploitation	Supply Chain Compromise	Sophisticated Botnets	Sophisticated Malwares	Cross-Platform Exploits	Mobile Platform Exploits	Social Engineering	Standard Botnets	Standard Malwares	DDoS Amplification	Automatic Hacking Toolkits	Misuse of Security Procedures
Highly Skilled	State-sponsored	Very High	●	●	●	●	●	●	●	●					
	Cyber Criminals	High				●	●		●	●					
Average Skill	Witting Insiders	Very High							●	●	●	●			
	Hacktivist/Cyber figthers	High								●	●	●	●	●	
	Unfunded Malicious	Medium							●	●	●	●			
Low Skill	Unwitting Insiders	Low								●					●

Fonte: Autor (2017)

Na habitual lógica de assimilação de conceitos da NATO na doutrina nacional, não é demais reiterar, enquanto tópico de controvérsia e crítica (IUM, 2016, pp. 45-46), que o conceito de ciberdefesa da NATO, pela amplitude reduzida que encerra, admissível do ponto

de vista da natureza da Aliança – de defesa coletiva –, é perigosamente minimizador e limitador no que às capacidades militares de um país se refere.

4.2.2. União Europeia

Representando cerca de 500 milhões de pessoas e com interesses e representação à escala mundial, também a UE enfrenta riscos e ameaças à segurança do seu ciberespaço que podem fazer perigar todo o seu modelo de funcionamento. Não é, pois, de estranhar que na área da ciberdefesa, considerada uma dimensão da cibersegurança (UE, 2016c, p. 6), tenham sido desenvolvidos esforços significativos, conforme apresentado na Figura 9.

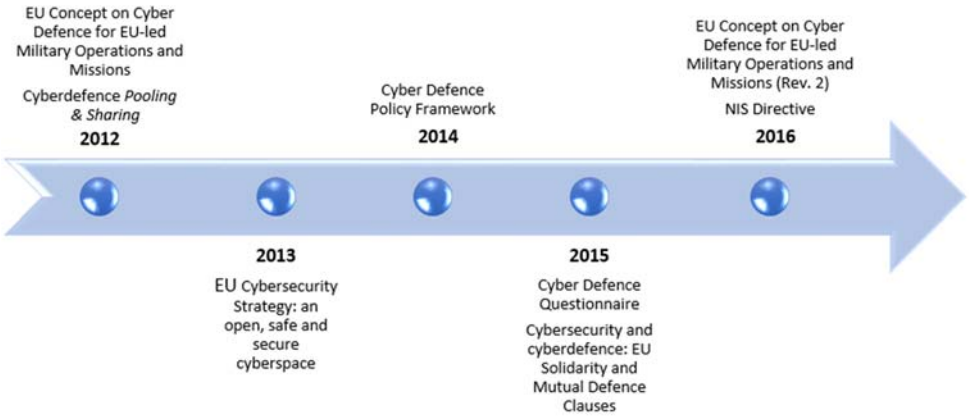


Figura 9 – Cronologia da ciberdefesa (UE)

Fonte: Autor (2017)

Relativamente à cibersegurança e ao impacto do ciberespaço nas diversas áreas, a UE (2016b, p. 16) releva a necessidade de se desenvolverem TIC que garantam a disponibilidade e integridade dos dados e, complementarmente, que assegurem a segurança do espaço digital europeu através da implementação de medidas específicas de segurança e normas de certificação de produtos e serviços digitais.

À luz dos indicadores e numa lógica de proporcionar contributos para o caso nacional, sistematiza-se informação relativa à ciberdefesa da UE (2016c), conforme Tabela 12.

Tabela 12 – Contributos (UE)

INDICADORES	CONTRIBUTOS
Doutrina	• A crescente dependência dos sistemas de armas e de C2 das TIC torna o ciberespaço uma dimensão crítica para o cumprimento das missões, devendo a sua proteção ser considerada aos diferentes níveis (estratégico, operacional e tático) e segundo o princípio da ciberdefesa coletiva. • O ciberespaço é um domínio crítico devendo ser considerado como novo ambiente operacional. • A ciberdefesa é entendida como resiliência e proteção dos sistemas baseados nas TIC. As operações ofensivas são enquadradas nas respostas ativas (*processos*) não sendo equacionadas capacidades ofensivas específicas.
Organização	• Elaboração de normas que sistematizem e automatizem os procedimentos de resposta a ciberataques. • Os processos e tecnologia devem estar orientados para uma postura preemptiva, consignada no princípio de que a questão não é determinar "se?" um ataque às nossas redes vai ser bem sucedido, mas "quando?" e "como?" vai ser executado. • Com o objetivo de apurar oportunamente sinais de alerta, os sistemas de deteção devem basear-se na observação prolongada do comportamento dos sistemas e do tráfego de rede. • Modelos de gestão de risco com base no princípio de que os objetivos no ciberespaço só podem ser atingidos após estimados as ameaças, vulnerabilidades e impacto, fatores limitados a um nível de aceitabilidade. • Incorporar na organização militar, aos diferentes níveis (estratégico, operacional e tático), células de ciberdefesa de modo a integrar a ciberdefesa no planeamento das operações. • Estruturas de *Security Operations Centre* em cada rede de missão de forma a monitorizar, analisar e avaliar as ciberameaças.
Treino	• O treino de procedimentos de cibersegurança deve ser feito a todos os níveis, desde logo ao nível individual nomeadamente abrangendo desde logo os aspetos mais básicos (ciber higiene). • Integração da ciberdefesa nos exercícios militares. • Educação orientada para a perceção comum da ciberameaça: minimizar diferenças entre os decisores e os técnicos de ciberdefesa.
Material	• Desenvolver a consciência de que a maior parte dos sistemas não incorporam requisitos de resiliência e resistência às ciberameaças pelo que importa implementar arquiteturas de segurança em função dos modelo de gestão de risco. • Perigos de manipulação na cadeia logística, nomeadamente pela presença de fornecedores não certificados. • Incorporação de tecnologias de análise de vulnerabilidades, *reverse engineering* e sistemas redundantes. • Implementação de arquiteturas de segurança multifronteiras com zonas desmilitarizadas. • Implementação de sistemas de deteção e de prevenção de intrusões.
Liderança	• Estrutura de governança implementada aos diferentes níveis de decisão, com a definição exata das funções de cada elemento. • Coordenação entre os diversos elementos atuantes no ciberespaço de modo a desconflituar ações e efeitos. • Promoção da cooperação e partilha da informação, nomeadamente com a NATO.
Pessoal	• Pese embora a perceção de que a cibersegurança é do âmbito tecnológico, o facto é que é o elemento humano a maior vulnerabilidade no ciberespaço (cerca de 95% dos incidentes).
Infraestruturas	• Implementação de estruturas com requisitos operacionais e funcionais conformes com as ciberatividades. • Implementação de *cyber ranges*. • Implementação de mecanismos e processos de troca de informação compatíveis com a velocidade e natureza dos processos no ciberespaço, nomeadamente entre os CERT e os CIRC.
Interoperabilidade	• Incorporação dos *standards* de ciberdefesa nas redes federadas de missão (FMN). • O crescente impacto do ciberespaço determina a necessidade da ciberdefesa ser considerada nos requisitos de interoperabilidade das capacidades militares.

Fonte: Autor (2017)

4.2.3. Brasil

A estrutura de segurança do ciberespaço (PRBrasil, 2008), função do nível da decisão e da natureza das ações a desenvolver, articula-se em quatro esferas de atuação (Figura 10), compreendendo as áreas da Segurança das CSI e Segurança Cibernética, da Defesa Cibernética e da Guerra Cibernética.

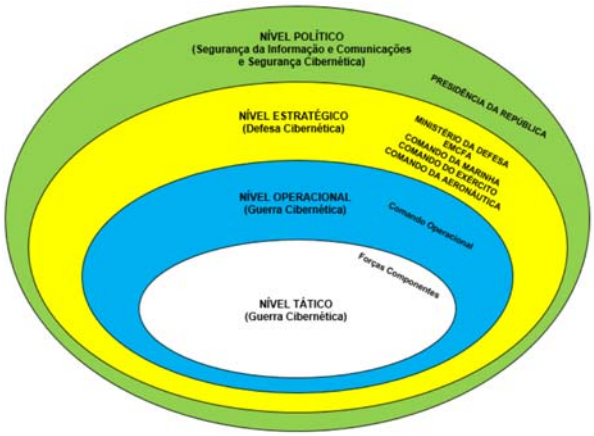


Figura 10 – Níveis de decisão das ações cibernéticas

Fonte: Ministério da Defesa (2014, p. 17)

No patamar militar, as responsabilidades situam-se ao nível estratégico[44] e ao nível operacional[45] (Figura 11), compreendendo respetivamente a Defesa Cibernética e a Guerra Cibernética (PRBrasil, 2011, p. 209).

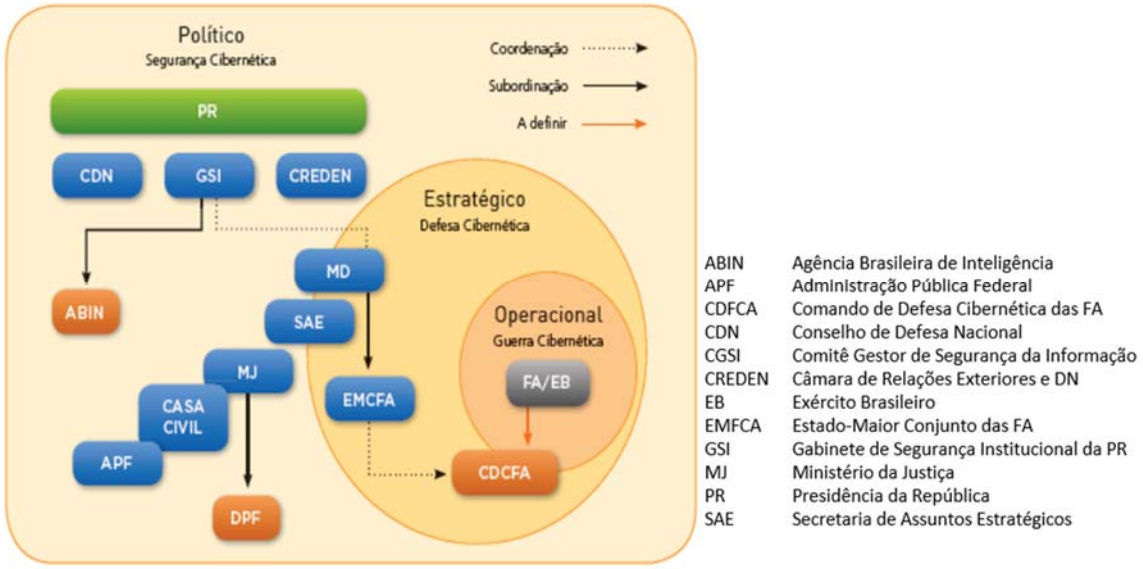


Figura 11 – Sistema de Segurança e Defesa Cibernética

Fonte: Adaptado de PR Brasil (2011, p. 204)

[44] Ações cibernéticas em situações de crise ou conflito armado.

[45] Ações cibernéticas, defensivas e ofensivas, relativas à preparação e emprego em operações, de qualquer natureza e intensidade.

Para este propósito, tem vindo a ser implementada uma estrutura da ciberdefesa (ver Figura 12) alicerçada em cinco vetores de desenvolvimento: infraestruturas; doutrina; treino operacional; investigação e desenvolvimento.

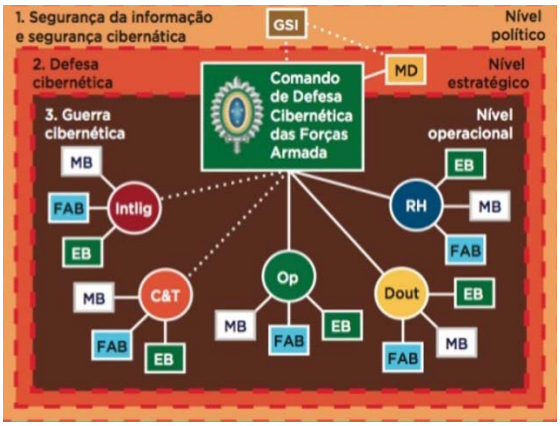


Figura 12 – Vetores de desenvolvimento da ciberdefesa

Fonte: PR Brasil (2011, p. 26)

Dos resultados apurados, cujos contributos essenciais se elencam na Tabela 13, conclui-se que o Brasil possui um Sistema de Segurança e Defesa Cibernética vocacionado maioritariamente para as operações e que se consubstancia, ao nível operacional, no Comando de Defesa Cibernético (Figura 13) e, ao nível tático, no Destacamento Conjunto de Guerra Cibernética e na Força Conjunta de Guerra Cibernética.

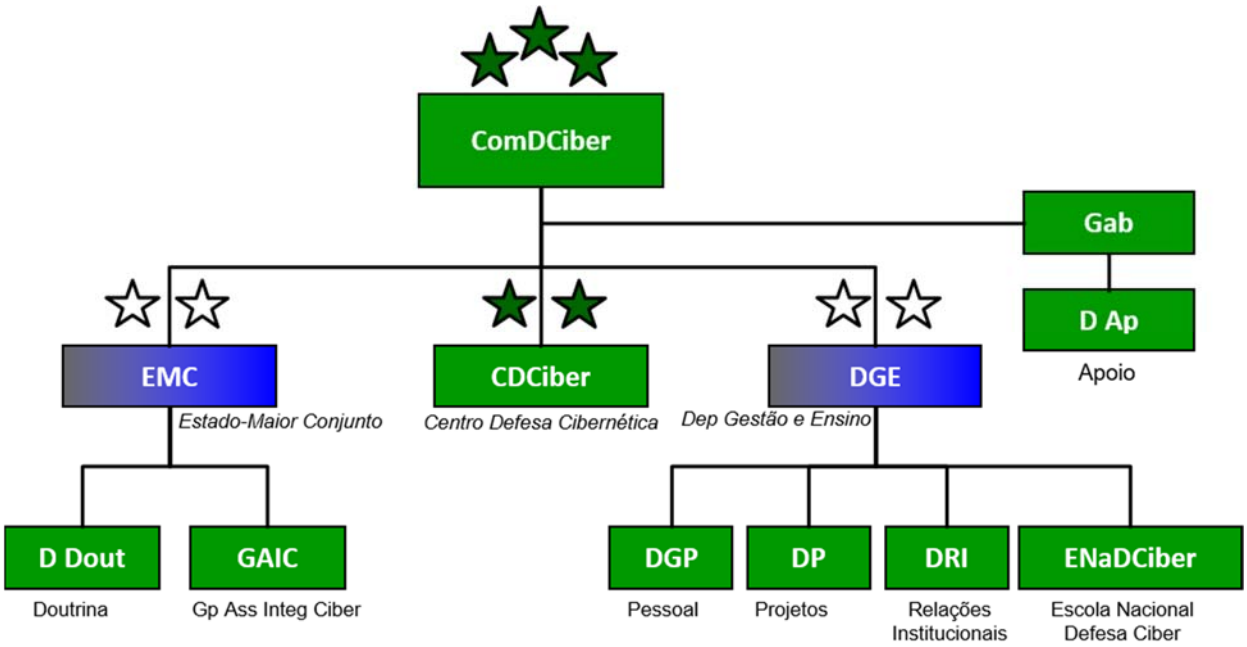


Figura 13 – Comando de Defesa Cibernética

Fonte: ComDCiber (2016)

Tabela 13 – Contributos (Brasil)

INDICADORES	CONTRIBUTOS
Doutrina	• Documentos principais: Estratégia de Segurança da CSI da Administração Pública Federal, Política Cibernética de Defesa, Estratégia Nacional de Defesa e Doutrina Militar de Defesa Cibernética. • Conceitos de ciberespaço, segurança cibernética, defesa cibernética, guerra cibernética, infraestruturas críticas e segurança da informação e comunicações (Apêndice A). • Competências da segurança cibernética: elaborar políticas de segurança cibernética; cooperação com órgãos congêneres de outros países; estabelecimento de normas e estratégias a nível nacional; relacionamento com as infraestruturas críticas nacionais; consciencialização da sociedade e prevenção e repressão do crime cibernético. • Objetivos Setoriais de Defesa (OSD): OSD 07 Utilização efetiva do espaço cibernético pelo Ministério da Defesa e a negação de tal uso contra os interesses da defesa e segurança nacionais. • Linhas de Ações Estratégicas de Defesa (cibernética): ASD 06 Implantar o Sistema Militar de Defesa Cibernética (SMDC). ASD 07 Promover a interoperabilidade do setor cibernético na Defesa Nacional. ASD 08 Criar e implantar o Comando de Defesa Cibernética. ASD 09 Criar e implantar a Escola Nacional de Defesa Cibernética. ASD 10 Implantar o Sistema de Homologação e Certificação de Produtos de Defesa Cibernética ASD 11 Desenvolver o Observatório Nacional de Defesa Cibernética. ASD 12 Capacitar e gerir recursos humanos necessários à condução das atividades do Setor Cibernético no âmbito da Defesa Nacional. ASD 13 Implantar o Sistema de Informações Seguras, com enfoque na área de segurança CSI. ASD 14 Contribuir para o fomento da pesquisa e do desenvolvimento de produtos de defesa . ASD 15 Contribuir para a produção do conhecimento de inteligência oriundo da fonte cibernética.
Organização	• **Comando de Defesa Cibernética** (ComDCiber). • **Centro de Defesa Cibernética** (CDCiber). • **Destacamento Conjunto de Guerra Cibernética** (DestConjDefCiber) em situação de não guerra. • **Força Conjunta de Guerra Cibernética** em situação de guerra. • Ao nível dos *processos* a desenvolver, os principais cenários e desafios à defesa cibernética são: 1. Capacitação de recursos humanos em quantidade suficiente para atender à procura; 2. Retenção de recursos humanos especializados; 3. Desenvolvimento de sistemas nacionais de defesa cibernética; 4. Número crescente de ameaças, com recursos humanos e financeiros aquém do necessário. • **Escola Nacional de Defesa Cibernética** (ENaDCiber).
Treino	• ----------
Material	• ----------
Liderança	• Reconhecida a necessidade mas ainda não foi desenvolvido nenhum programa específico.
Pessoal	• Não têm uma especialidade específica para a ciberdefesa. Consideram como requisitos ter conhecimentos na área da ciência da computação, segurança de redes e das CSI. • Admissão é efetuada ao nível dos ramos das FA. • Não incorporam operadores civis na estrutura de defesa cibernética.
Infraestruturas	• ComDCiber (Brasília) com dependência do Comando do Exército (Dep. de Ciência e Tecnologia). • DestConjDefCiber (Força Conjunta).
Interoperabilidade	• *Processos* e *tecnologias* orientados para: Atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias; Cooperar na produção de informações (*cyber intelligence*); Cooperar com a Segurança Cibernética; Cooperar com o esforço de mobilização para assegurar a capacidade de Defesa Cibernética; Realizar ações contra oponentes mais fortes, dentro do conceito de guerra assimétrica.

Fonte: Autor (2017)

4.2.4. Espanha

A *Estrategia de Ciberseguridad Nacional* (Gobierno de España, 2013) fixa como objetivo global, assegurar o uso seguro das CSI e as capacidades de prevenção de fortalecimento, defesa, deteção e resposta a ataques cibernéticos.

Ao nível militar e numa primeira fase, Espanha edificou a capacidade de ciberdefesa orientada para a segurança das CSI, tendo posteriormente adotado uma estrutura capacitada para responder a ameaças ou agressões veiculadas pelo ciberespaço que possam afetar o país (Ministerio de Defensa, 2014, p. 84094).

Assumindo o paradigma do ciberespaço como domínio operacional, foi edificado o *Mando Conjunto de Ciberdefensa* (MCCD), na dependência do *Jefe de Estado Mayor de la Defensa*, conforme Figura 14.

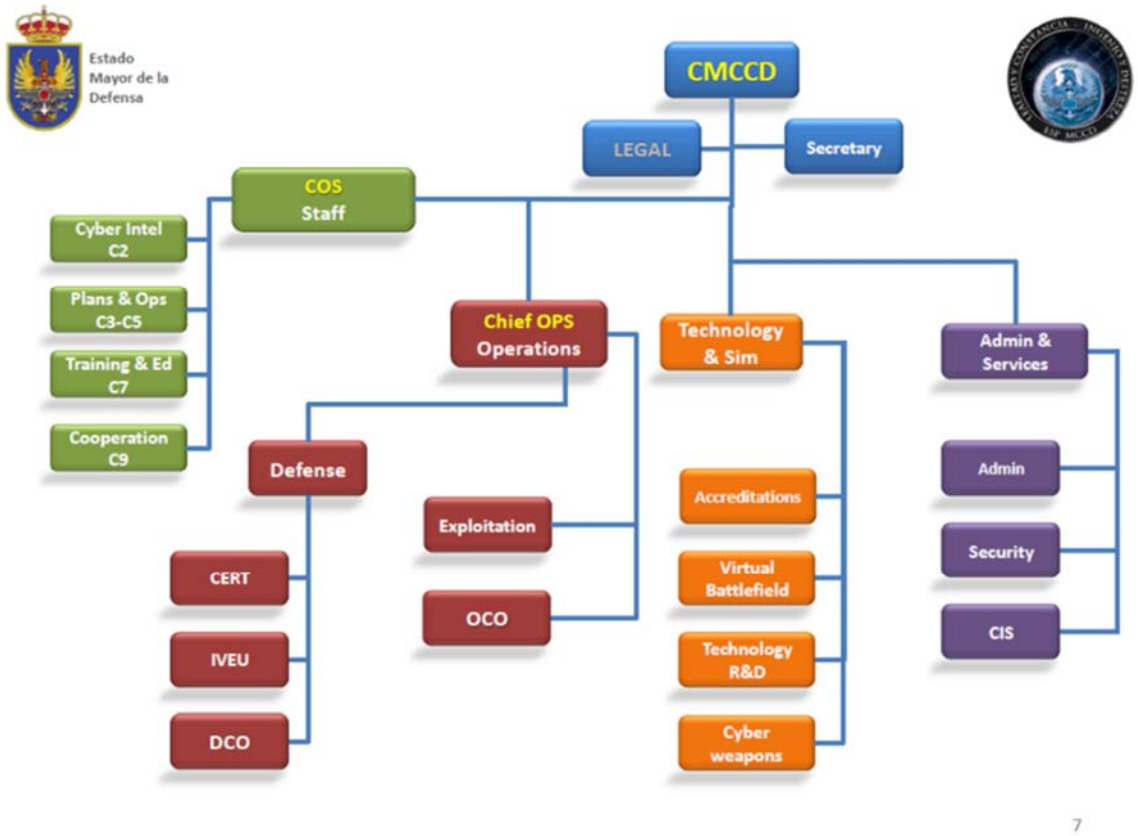


Figura 14 – Estrutura do MCCD

Fonte: MCCD (2016b, p. 7)

Este comando, que se articula em diversas áreas funcionais, encerra as seguintes atribuições (MCCD, 2016a) principais:

– Dirigir e coordenar, na defesa cibernética, a atividade dos CIRC das FA;

– Assegurar a resposta oportuna, legítima e proporcional no ciberespaço a ameaças ou ataques que possam afetar a defesa nacional;

– Definir, dirigir e coordenar as ações de sensibilização, formação e treino na área da ciberdefesa.

Como comando da componente ciber e para efeitos operacionais, o MCCD está integrado na força conjunta (Figura 15).

Figura 15 – Estrutura da Força Conjunta

Fonte: Autor (2017)

Registe-se ainda o facto da ciberdefesa espanhola, que se encontra em adiantado grau de implementação, ter assumido como principal desafio o ciberespaço como domínio operacional (MCCD, 2016a, p. 2.3.4), tendo para o efeito integrado as ciberoperações nas operações conjuntas e combinadas, com resultados visíveis ao nível da eficiência das restantes capacidades militares.

Em função dos dados recolhidos e de acordo com o MA, foi possível identificar contributos que se encontram sistematizados na Tabela 14.

Tabela 14 – Contributos (Espanha)

INDICADORES	CONTRIBUTOS
Doutrina	• *Estratégia de Ciberseguridad Nacional* é o documento que integra todos os aspetos da segurança do ciberespaço nacional. • Conceitos utilizados: **Ciberespaço**: domínio global e dinâmico composto pelas infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações e sistemas de informação. **Cibersegurança**: conjunto de ações com o objetivo de assegurar o funcionamento das redes e sistemas que constituem o ciberespaço, garantindo a deteção e resposta a intrusões, a reação e recuperação de incidentes e a preservação da confidencialidade, disponibilidade e integridade da informação. **Ciberdefesa**: conjunto de meios para alcançar e executar medidas defensivas contra ciberataques de modo a contrariar ou mitigar os seus efeito e preservar e restaurar a segurança das CSI. Para o efeito compreende Medidas de Defesa Interna, Medidas de Recuperação e Medidas de Defesa Externa.
Organização	• Órgãos de segurança do ciberespaço: Conselho Nacional de Cibersegurança (representantes de 13 ministérios); Centro Criptológico Nacional; Administração Pública através do Instituto Nacional de Cibersegurança (CERT Gov); Ministério do Interior (domínio público e privado) através das infraestruturas críticas, cibercrime e ciberterrorismo; Ministério da Defesa através do **Comando Conjunto de Ciberdefesa** (MCCD). • Linhas de ação estratégica (Goberno de España, 2013, p. 31): 1. Capacidade de prevenção, deteção, resposta e recuperação de ciberameaças. 2. Segurança dos sistemas de informação e telecomunicações da administração pública. 3. Segurança dos sistemas de informação e telecomunicações de apoio às infraestruturas críticas. 4. Segurança e resiliência das TIC do setor privado. 5. Capacidade de investigação e combate ao cibercrime e ciberterrorismo. 6. Cultura de cibersegurança. 7. Compromissos internacionais.
Treino	• A ciberdefesa está incluída na formação de base nas academias militares, Curso de Estado-Maior e na Escola Militar de estudos Jurídicos. • Cursos conjuntos de ciberdefesa: Básico (Marinha), Avançado (Exército) e Especializado (Força Aérea). • Também o Centro de Estudos Superiores de Defesa (CESEDEN) tem programas de ciberdefesa nos currículos dos cursos que ministra.
Material	• A ciberdefesa tem um orçamento específico ao nível do Estado-Maior da Defesa.
Liderança	• Está em preparação um programa para adaptação das lideranças ao novo ambiente operacional. O processo de tomada de decisão está estratificado: político (governo), estratégico (CEMGFA), operacional (comandante do Comando de Operações) e ao nível tático (comandante do MCCD).
Pessoal	• Não existe uma especialidade orientada para a ciberdefesa nem uma carreira autónoma. • Não existe um processo de incorporação diferenciado, estando este ao nível dos ramos das FA. • No sentido de colmatar lacunas na obtenção e especialistas utilizam um modelo de reserva voluntária para incorporar civis na ciberdefesa.
Infraestruturas	• O MCCD: **Depende do CEMGFA.** Pertence ao Estado-Maior Conjunto (EMAD). Integra a estrutura operacional das FA como um **comando de componente** (CCC).
Interoperabilidade	• Ao nível dos processos o MCCD é responsável por: 1. Desenvolver, dirigir, executar e controlar as políticas de segurança das CSI do MD. 2. Dirigir e coordenar diretamente a atividade dos CIRC da Marinha, Exército e Força Aérea (sistemas corporativos e conjuntos). 3. As CSI do MD e outras redes e sistemas especificamente atribuídos e ações de resposta.

Fonte: Autor (2017)

4.2.5. República da Coreia

Similarmente a outros exemplos, a edificação do sistema de ciberdefesa na ROK teve origem num órgão na área da segurança da informação (CERT), tendo posteriormente evoluído para uma organização complexa, no âmbito das ciberoperações, adaptando assim a organização militar ao novo paradigma de objetivos que, do domínio exclusivo das TIC, passou também a abranger as IC (Young-ju, 2016, pp. 223-224).

Conforme Figura 16, o modelo coreano segmenta o ciberespaço em três setores interdependentes – privado, público e da defesa – considerando que perturbações nos setores público ou privado impactam negativamente na defesa (Young-ju, 2016, p. 227), considerando que:

– A afetação de serviços essenciais influi na capacidade de projeção e de C2 das capacidades militares;

– A afetação dos sistemas de gestão de combate impacta na capacidade militar;

– A afetação ou a paralisação do governo ou das instituições públicas criam confusão social, que pode limitar o emprego das capacidades militares.

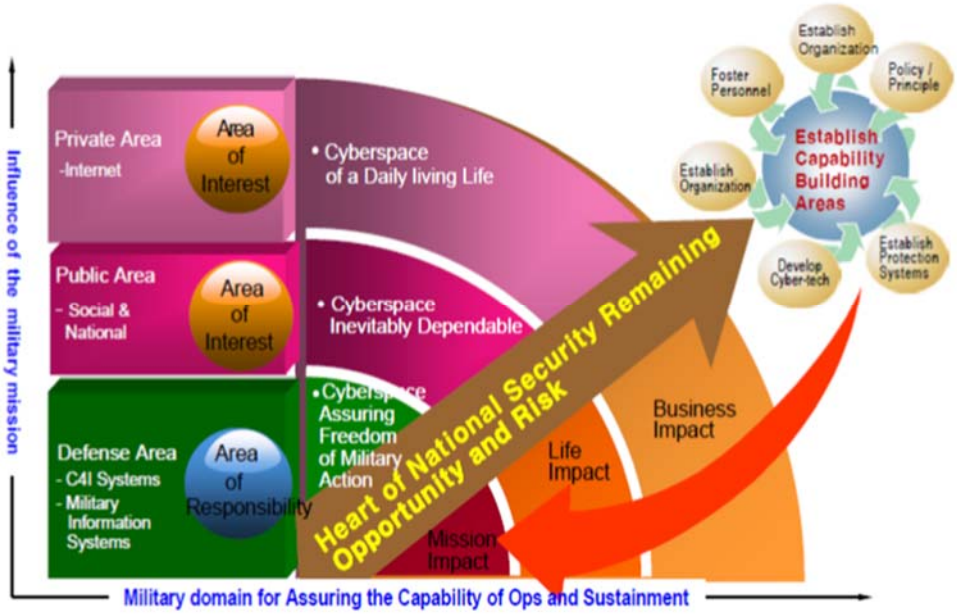


Figura 16 – Impacto operacional do ciberespaço (ROK)

Fonte: Young-ju (2016, p. 229)

Da análise aos elementos recolhidos e cujos resultados se apresentam na Tabela 15, pode-se concluir que, empiricamente, a operacionalização da capacidade de ciberdefesa se articulou em duas fases distintas, em razão da natureza das missões que foi cumprindo. Segundo Kshetri (2016, p. 176), a primeira fase[46] visou essencialmente a proteção das redes e o apoio às OI, claramente na esfera da cibersegurança, sendo a segunda fase[47] direcionada para a projeção de força no/através do ciberespaço, suportada no desenvolvimento de armas cibernéticas, envolvendo a produção de efeitos cinéticos. Em termos organizacionais da ciberderfesa (IISS, 2015, p. 179), constituíram-se as seguintes estruturas principais:

– O *Cyber Warfare Command*, subordinado ao Ministério da Defesa (MD), com a missão de defender as redes, sistemas e a informação da Defesa.

– O *Cyber Warfare Centre*, na dependência do comando das FA, com a missão de conduzir OC.

– Capacidades operativas de ciberdefesa na dependência dos ramos.

Aos níveis operacional e genético, a prossecução da capacidade de ciberdefesa gizou-se pelas seguintes linhas de ação (Young-ju, 2016, pp. 229-230):

– Implantação de uma organização que assegure a transição de uma estrutura tipo CERT para uma estrutura capaz de executar OC.

– Elaboração de legislação e de regras de empenhamento que agilizem a transição do estado de paz para os estados de exceção.

– Edificação de um comando de ciberdefesa capaz de executar OC nos três segmentos do ciberespaço.

– Inclusão, nos comandos das componentes militares e dos ramos das FA, da capacidade de integrarem as ações do Comando de Ciberdefesa.

[46] 2010-2014.
[47] Desde 2015.

Tabela 15 – Contributos (ROK)

INDICADORES	CONTRIBUTOS
Doutrina	• Estratégia de cibersegurança publicada em 2010. • Capacidades cibernéticas desenvolvidas numa lógica de capacidades assimétricas. • O sistema de ciberdefesa (RoK) teve origem numa estrutura orientada primariamente para a proteção da informação tendo evoluído para um sistema orientado às operações no ciberespaço. • Conceito de operações do ciberespaço: qualquer processo que altere de forma maliciosa ou intencional um ou mais elementos do ciclo de vida do ciberespaço. Em termos dos processos a desenvolver e das responsabilidades a alocar, o sistema de defesa estratifica o ciberespaço em três setores interconectados: setor privado (internet); setor público (infraestruturas críticas) e setor da Defesa (intranet militar, redes de operações, sistemas de armas e sistemas de C2). • Sistematização das operações no ciberespaço em **ofensivas**, **defensivas** e em **rede.** Seis ações: 1. Ciber ataque: neutralizar, destruir ou alterar os sistemas alvo; 2. Ciber defesa: resposta ativa defensiva podendo incluir o contra ataque; 3. Ciber ISR: informação sobre as ciberameaças e ciberaquisição de objetivos; 4. Ciber operações em redes: na área da cibersegurança contribuindo para a proteção das CSI; 5. Ciber preparação do ambiente operacional: avaliação da situação (riscos e ameaças); 6. Ciber sustentação: pesquisa, desenvolvimento, teste e análise forense.
Organização	• O ***Cyber Warfare Command*** , ao nível do MD (defender as redes, sistemas e informação na área da Defesa). • O ***Cyber Warfare Centre***, na dependência do JCS, para a área da ciberdefesa. • **Estruturas táticas** de ciberdefesa em cada ramo. • O impacto do ciberespaço enquanto domínio militar deve ser avaliado ao nível operacional e da sustentação nos três setores, devendo as capacidades serem desenvolvidas considerando as seguintes linhas de orientação (Young-ju, 2016, pp. 229-230): 1. Estabelecimento de legislação e regras de empenhamento e operação de modo a desconflituar a ação dos vários atores e manter uma postura ativa e célere na transição para o estado de crise ou guerra. (*cyber threat information sharing*). 2. O RoK *Cyber Command* (RCC) deve garantir a liberdade de ação das FA no ciberespaço e simultaneamente assegurar a integração das cibercapacidades nas ações de guerra convencional (integração nas operações militares e sincronizar operações nas três áreas). 3. Requisito operacional do RCC: executar operações no ciberespaço independentemente e em coordenação com outras entidades no quadro de responsabilidades e missões atribuídas. 4. Os comandos das componentes militares e dos ramos das FA devem ter a capacidade de integrarem as ações do RCC evitando postura e limitações tradicionais dos CIRC.
Treino	• Capacidade ciber integrada nas operações militares (*social networking* e *social media websites).*
Material	• Tipologia de alvos dos ciberataques: do domínio exclusivo das TIC para as infraestruturas críticas. • Inclusão ou não da internet no ciberespaço (abrangência voluntária em função da decisão humana, subsistindo outros aspetos do ciberespaço como as intranets, sistemas de armas e C2. • Orçamento 2010 a 2017 de 8100 M€ (Kshetri, 2014, p. 195).
Liderança	• Unidade de esforços e adaptação do processo de tomada da decisão. • As operações no ciberespaço, na dimensão processos, orientaram-se, numa primeira fase, para o apoio às operações de informação; numa segunda fase, em curso, para o desenvolvimento de ciberarmas direcionadas para a capacidade nuclear e balística da Coreia do Norte.
Pessoal	• Pessoal militar e civil nas estruturas de ciberdefesa. • Incorporar cerca de 5000 ciberespecialistas no período 2010 a 2017 (Kshetri, 2014, p. 195). • O efetivo *do Cyber Warfare Command* a no final do período 2013-2017 é de 1000 pessoas.
Infraestruturas	• Requisitos operacionais no desenvolvimento da capacidade de ciberdefesa: 1. Garantia da missão. Para tal concorre o processo de análise de risco integrado prolongado no tempo, que contribua para a identificação dos ativos críticos e gerir o risco associado de modo a garantir a eficiência operacional das capacidades criticas da Defesa. As operações no ciberespaço como multiplicador de força por integração com as operações nos domínios físicos. 2. Criar efeito de dissuasão que desencoraje adversários a executarem ataques cibernéticos.
Interoperabilidade	• Nos *processos* e da *tecnologia* associada, prioridade para a partilha de informação (*cyber intel*). • Sincronização de processos de modo a desconflituar os ciberefeitos. • Criação do *Defense Ciber Cooperation Working Group* entre os EUA e a RoK, nas áreas da estratégia, doutrina, treino e pessoal.

Fonte: Autor (2017)

Por último e nas dimensões *processos* e *tecnologia*, é de referir que, no âmbito da proteção dos sistemas e em função da análise de risco, a ROK implementou um sistema multicamada, adaptativo e flexível[48] (Lee & Kang, 2015, p. 3), assente numa arquitetura ternária (ver Figura 17) compreendendo as áreas da operação, dos sistemas e da tecnologia.

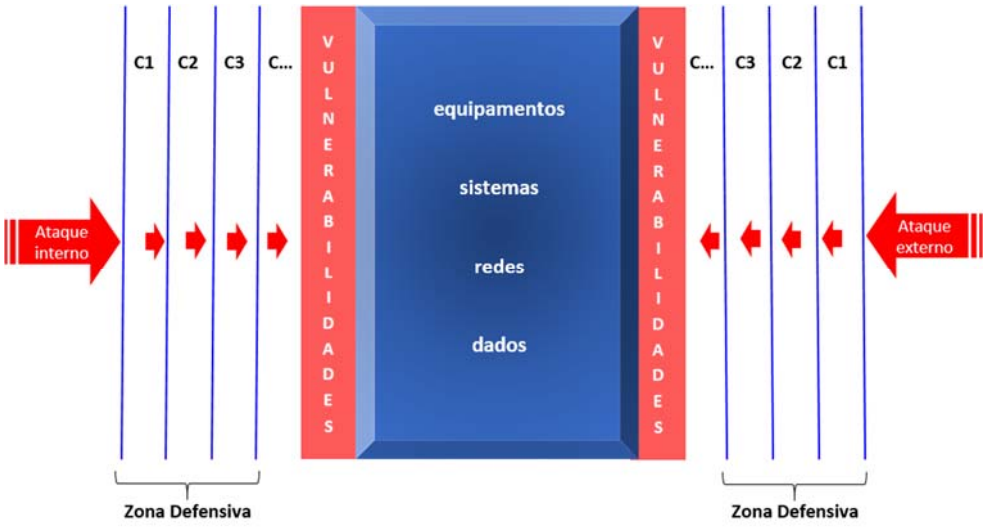


Figura 17 – Defesa multicamada

Fonte: Adaptado de Lee e Kang (2015, p. 8)

4.3. Análise por dimensões

Como últimos elementos da análise dos dados recolhidos, aqui maioritariamente obtidos por via da pesquisa bibliográfica, enunciam-se alguns contributos nas dimensões do MA.

4.3.1. Pessoas

O desafio do ciberespaço impõe a consequente adaptação das FA, promovendo desde logo nas pessoas – recurso organizacional mais importante– uma mudança relativamente à área de operações, ou seja, passar de uma postura analítica baseada em objetos tangíveis, típicos dos domínios físicos, para uma postura centrada agora em objetivos intangíveis (Loerch, 2016, p. 31) onde é exigido um considerável grau de abstração. Preparar as FA para este AO, de acordo com Seffers (2016, p. 48), exige um estilo de liderança que cultive a adoção de novos procedimentos, abandonando a tradicional perceção de que as redes (sentido restrito de ciberespaço) são um serviço, em detrimento da perceção das redes como

[48] Que assegura respostas, na maioria das vezes automatizadas, aos diferentes vetores de ataque.

plataforma de operações, onde podem ser alcançados objetivos ou, por via da referida transversalidade, concorrer para produzir efeitos noutros domínios. Segundo Ackerman (2015c, p. 19), entender o ciberespaço como domínio da guerra implica olhar para as cibercapacidades como sistemas de armas, do nível operacional ao nível tático, exigindo a implementação de mecanismos de coordenação que, em função das características do ciberespaço, terão de obedecer a uma lógica do processo da decisão diferenciada da dos restantes domínios.

O MA, quando aplicado às organizações com responsabilidades na segurança do ciberespaço, identifica claramente a dimensão pessoas como a mais crítica para o sucesso, constatação enfaticamente sublinhada pelo Secretário Geral da Segurança Interna dos EUA (AFCEA, 2016a, p. 9), ao considerar o recrutamento de talentos de topo na área ciber como tarefa crucial para o bom cumprimento da missão. Em complemento ao pessoal militar, a necessidade de recorrer a civis nesta área é também objeto de reflexão ao mais alto nível das FA, considerando Monteiro (2017, p. C1) que, especificamente na componente defensiva, a utilização de operadores civis integrados na estrutura militar da unidade de cúpula da ciberdefesa poderá colmatar as lacunas existentes, permitindo assim focar os recursos militares nas tarefas intrínsecas às operações militares no ciberespaço.

Pese embora ser ponto assente que é entre os denominados *millennials*[49] que se encontram as pessoas melhor preparadas para operar neste ambiente, embora no caso nacional escasseiem os necessários fatores de aliciamento, importa reter que, paradoxalmente e de acordo com o publicado recentemente (AFCEA, 2016b, p. 9), estes representam também a maior fonte de ciberrisco, pela enorme disponibilidade e apetência para incorporarem no quotidiano novas tecnologias e comportamentos em rede que privilegiam a rapidez e a universalidade em detrimento da segurança e mesmo da confidencialidade.

A necessidade de estender as ciberoperações aos mais baixos escalões do dispositivo de forças é considerada como fator determinante para o sucesso no ciberespaço, tendo o Exército Americano (Jontz, 2016a, p. 21) constituído equipas de combate capacitadas com as valências da ciberdefesa, GE, OI, operações em rede e informações, vigilância e reconhecimento. Como métrica de referência nos EUA (Jontz, 2016a, p. 23), e para uma brigada com efetivo de 4.000 homens, aponta-se o efetivo de 40-50 cibercombatentes[50].

[49] Geração nascida nos anos 1977 a 1994.
[50] Correspondente a cerca de 1% do efetivo da força.

4.3.2. Processos

À semelhança do advento da aviação e, posteriormente, das redes de CSI, também a emergência do ciberespaço determinou uma evolução do AO, percebido como "conjunto de condições, circunstâncias e fatores influenciadores que afetam o emprego de forças militares e influenciam as decisões" (Exército, 2012, p. 17). Segundo o Army Cyber Command (2013, p. 3), a configuração do novo AO (ver Figura 18) carateriza-se pelo incremento exponencial da taxa de ações/impactos na área de operações bem como na convergência dos elementos dimensão física–fator humano–ciberespaço.

Figura 18 – Ambiente operacional

Fonte: Adaptado de Army Cyber Command (2013, p. 3)

Um dos maiores desafios que se colocam ao planeamento das OC reside na dificuldade de transposição dos procedimentos de ciberdefesa, que são de natureza iminentemente técnica, para os ditames do planeamento operacional, nomeadamente na decomposição dos objetivos estratégicos visando identificar os centros de gravidade e, assim, determinar as potenciais vulnerabilidades a explorar. Para Barber (2015, p. 3), a natureza complexa e dinâmica do ciberespaço requer uma análise técnica e um planeamento que não são acomodados pela doutrina existente. Para mitigar esta insuficiência, refere ainda este autor a mais-valia da utilização de modelos de transposição, por semelhança com os processos que ocorrem nos domínios físicos. Somente com caráter ilustrativo da transposição dos impactos

cibernéticos em efeitos mais visíveis para o planeamento militar, a Figura 19 estabelece de forma genérica o paralelo entre o processo de aquisição de objetivos numa operação militar tradicional e os processos típicos do ciberespaço.

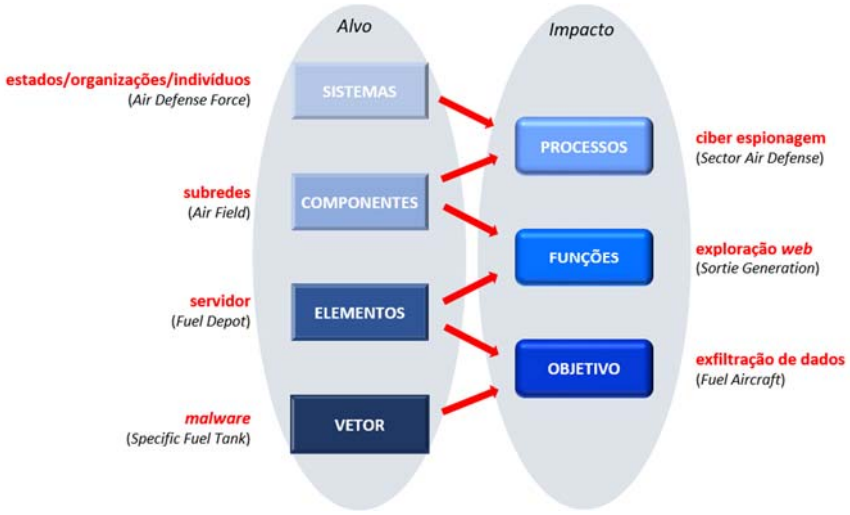


Figura 19 – Modelo de aquisição de objetivos

Fonte: Adaptado de Barber et al. (2015, p. 5)

Relativamente ao indicador doutrina e complementarmente aos aspetos já mencionados, parece existir unanimidade no reconhecimento das OC como sustentáculo de uma nova capacidade militar. Segundo o diretor da *Defense Information Systems Agency* (Lynn, cit. por Jontz, 2016d, p. 40), o desafio na modernização das FA dos EUA passa por incorporar a capacidade de manobrar no EM e no ciberespaço, executando missões defensivas e ofensivas. Também a Austrália, e muitos outros exemplos haveria, através do seu primeiro-ministro (Turnbull, cit. por Slocombe, 2016, p. 46), publicitou a sua postura relativa às ameaças cibernéticas, afirmando que o Governo encara, como resposta, o recurso a diversos tipos de coação considerando, nomeadamente, a utilização uma capacidade cibernética ofensiva.

4.3.3. Tecnologias

O custo reduzido de acesso ao ciberespaço, a par da rápida evolução das TIC, favorece, em larga escala, a utilização de ferramentas operativas iminentemente comerciais. No quadro da avaliação do risco, uma das maiores vulnerabilidades reside na utilização destes equipamentos, que, não estando sujeitos ao tradicional controlo da cadeia logística do

material bélico, poderão constituir vetores de intrusão e pôr assim em causa a segurança das operações (Ackerman, 2015d, p. 28).

4.3.4. Estruturas

No exercício da soberania no ciberespaço e na lógica do que acontece com as demais componentes, em que se procura a unidade de comando, os sistemas são operados, orientados, protegidos e defendidos, ao mesmo tempo em que se negam as capacidades adversárias. A necessidade de integrar as operações de segurança e as operações defensivas sob um único comando (Hawkins cit. por Ackerman, 2015c, p. 20) foi uma preocupação na definição da estrutura de ciberdefesa dos EUA. Subjacente à edificação de capacidades operativas está a premissa de que a superioridade no ciberespaço, ou o seu controlo global, são objetivos tecnicamente impossíveis de alcançar. Outrossim, é definir-se como finalidade a obtenção de superioridade e controlo do ciberespaço em determinados elementos críticos das operações, e, apenas, num determinado lapso temporal (Stytz & Banks, 2014, p. 55).

Como elemento enformador das valências a incorporar face à tipologia de operações a executar, é importante definir o nível da ameaça, sendo este entendido por Monteiro (2017, pp. C-1) como inaceitável e como tal exigindo uma postura ofensiva das FA, quando coloque em causa a soberania nacional no ciberespaço, a livre atuação no mesmo ou ponha em risco os princípios básicos da confidencialidade, integridade e disponibilidade associados às CSI das FA.

4.4. **Síntese conclusiva**

A evolução do AO, a tipologia de riscos e as ameaças associadas determinam novos desafios à segurança e defesa dos estados a que as FA não podem ser indiferentes. No propósito de identificar elementos de informação que possam constituir contributos supletivos para a operacionalização da capacidade de ciberdefesa nacional, foram analisados, nas respetivas dimensões e indicadores, sistemas de ciberdefesa de países e organizações internacionais, bem como bibliografia considerada de referência.

Como elemento conclusivo transversal às diferentes realidades analisadas, registe-se o facto de o ciberespaço, enquanto promotor de progresso, mas também vetor de uma nova expressão da conflitualidade, determinar uma adaptação das estruturas de defesa dos estados e logicamente das FA, mormente pelo aparecimento de uma nova capacidade militar – a ciberdefesa. Na dimensão processos e consequência do novo paradigma de alvos, note-se a mudança dos objetivos, anteriormente centrados na CSI e agora mais direcionados para objetivos mais tangíveis, procurando afetar IC e serviços essenciais. Consequência desta

realidade nos processos militares, sublinha-se a necessidade de se proceder à conceptualização do ciberespaço como domínio operacional, sistematizando o espectro de operações por incorporação de diversas tipologias de ações e efeitos afins, compreendendo a bivalência das ciberoperações, enquanto multiplicador do potencial de combate, em apoio aos demais domínios, ou projetando força para alcançar objetivos no ciberespaço, não descurando a hipótese de se produzirem efeitos cinéticos.

Transversal aos modelos estudados, com especial impacto na organização e nos processos, verifica-se a autonomização da ciberdefesa como componente das operações, determinando, ao nível ao nível estratégico-operacional a edificação do respetivo comando de componente, a reformulação das células J6 dos estados-maiores e, ao nível tático, a criação de equipas de ciberdefesa.

Na dimensão pessoas, foi visível a necessidade de sensibilizar as lideranças militares para o impacto do ciberespaço nas operações militares, bem como a necessidade de ajustar o processo de decisão às novas dinâmicas, nomeadamente pela normalização de procedimentos que automatizem as reações aos ciberincidentes. Face à complexidade dos processos que atingem a área de operações, constatou-se a necessidade de formação substancialmente exigente e diferenciada, transparecendo a necessidade de desempenhos muito prolongados para a aquisição das competências desejáveis, situação que recomenda, no nível estratégico-operacional[51] e nas atividades de cibersegurança e de sustentação dos sistemas, a presença de pessoal civil, alocando ao pessoal militar as tarefas de direção, planeamento e operação dos sistemas táticos de ciberdefesa.

Uma última referência – processos e tecnologia – para a interiorização do princípio da impossibilidade de obtenção de superioridade prolongada no ciberespaço e para a necessidade de ajustar o planeamento operacional em função das capacidades cibernéticas serem percebidas como sistemas de armas com capacidade, no limite, de produzir efeitos cinéticos.

Da análise efetuada, consubstanciada na informação sistematizada, foi possível identificar contributos para a edificação da capacidade de ciberdefesa nas dimensões críticas das organizações de segurança do ciberespaço, considerando-se assim validada a H3, respondida a QD3 e atingido o OE3.

[51] Operação dos sistemas.

Conclusões

Introdução

A observação atenta dos fenómenos do ciberespaço que impactam na segurança dos estados permite identificar como denominador comum a transversalidade dos efeitos das ações hostis, entendidas como afetando os vários domínios da sociedade contemporânea. Considerados nos seus aspetos caraterizadores e muitas vezes específicos, os riscos veiculados pelo ciberespaço enquadram-se nas grandes preocupações securitárias dos países, de que Portugal não deverá eximir-se.

O desenvolvimento de eventuais atividades ou operações maliciosas que possam pôr em causa a soberania e a defesa do Estado português, irão provavelmente reconhecer o potencial de utilizar ataques cibernéticos para condicionar a confiança na integridade e na confidencialidade da informação que é transmitida, processada e armazenada, abalando os alicerces da atual sociedade da informação.

O presente trabalho teve como objeto de investigação a ciberdefesa. Pese embora este termo não se encontrar ainda definido no quadro conceptual nacional, o conceito geral que assistiu à investigação foi o de entender a ciberdefesa como uma capacidade militar, englobando os processos e recursos necessários para que as FA, também no ciberespaço, sejam capazes de cumprir as missões que lhes estão atribuídas.

Sumário com as grandes linhas do procedimento metodológico

Como elemento de referência para a elaboração deste trabalho, foi fixado como OG identificar contributos para a edificação de uma capacidade militar que assegure a atuação eficaz das FA no ciberespaço, tendo a pesquisa sido orientada pela procura de informação que concorra para a operacionalização de uma capacidade que habilite as FA a executarem operações no ciberespaço. Para a sua prossecução, a investigação orientou-se segundo três linhas de ação: avaliar o impacto nas FA do ciberespaço como domínio operacional; avaliar o estado da ciberdefesa nas FA na ótica de uma capacidade militar; identificar elementos de informação em sistemas de ciberdefesa consolidados que possam constituir contributos para a implementação da capacidade nacional.

Do ponto de vista metodológico, o estudo baseou-se num raciocínio hipotético-dedutivo, adotando-se uma estratégia de investigação essencialmente qualitativa, procurando buscar contributos em organizações internacionais de que Portugal é membro e em sistemas de ciberdefesa já consolidados. O desenho da pesquisa, de natureza empírica e descritiva, foi essencialmente do tipo estudo de caso, em que se procurou compreender a

ciberdefesa através de uma perspetiva interpretativa, considerando o ponto de vista dos entrevistados, a análise documental das orientações e recomendações da NATO e da UE, bem como os padrões encontrados nas capacidades de ciberdefesa do Brasil, de Espanha e da ROK.

Atendendo aos elementos críticos das organizações de segurança do ciberespaço e aos vetores de desenvolvimento de capacidades militares, definiu-se um modelo de análise articulado em dimensões (pessoas, processos, tecnologia e estruturas) que, sendo transversais a todo o estudo, constituíram elementos informadores das conclusões, de que aqui se relevam os aspetos julgados principais.

Avaliação dos resultados obtidos

Conforme expresso no OE1, a primeira linha de investigação centrou-se nas implicações do ciberespaço ter sido considerado domínio operacional, procurando avaliar a capacidade de as FA responderem aos novos desafios deste novo domínio da guerra. Como elemento essencial da análise, pôde-se concluir que considerar o ciberespaço como domínio operacional implica substantivamente uma mudança do paradigma da ciberdefesa, por evolução de um conceito tradicionalmente orientado para a guerra da informação – inestimável contributo para as OI – para um conceito mais abrangente, de produtor ou multiplicador de força, orientado para as operações, visando objetivos no, ou através do, ciberespaço, não descurando a possibilidade de incluir efeitos cinéticos. Para tal desiderato, identificou-se como indispensável a existência de um órgão que, ao nível estratégico-operacional, incorpore as valências de comando de componente e, ao nível tático e necessariamente inseridas nos ramos, se estabeleçam estruturas que, de forma criteriosa e integrada, capacitem as FA a combater no novo domínio. Também ao nível doutrinário foram identificadas implicações que importa fazer refletir nas FA, nomeadamente a necessidade de se proceder à integração das disciplinas que atuam no EEM (GE e OC) e, sobretudo, de começar a preparar as FA para as denominadas operações multidomínio. Esta nova conceptualização operacional vem determinar uma nova *revolution in militar affairs*, numa lógica evolutiva do conceito de operações conjuntas, por via da incorporação de elevados níveis de interoperabilidade e sofisticação tecnológica, em que ações específicas num domínio, sustentadas em tecnologia orientada, podem desencadear atividades síncronas noutros domínios que concorram para o efeito pretendido.

Subjacente ao OE2, a segunda linha de investigação procurou avaliar a ciberdefesa nas FA no contexto da implementação de uma capacidade militar, pretendendo aferir o efetivo

estado de implementação, atendendo aos indicadores do MA. Da análise efetuada, pôde-se concluir da adequabilidade do quadro normativo existente, que, no âmbito da ciberdefesa, fixa já competências às FA compatíveis com o conceito de ciberdefesa vocacionado para as operações militares no ciberespaço. No entanto, diga-se surpreendentemente, por precisamente constituir a estratégia militar, importa referir a desadequação do atual CEM, por não incorporar a dimensão ciberespaço como domínio operacional, permanecendo ainda na anterior postura da ciberdefesa orientada para a segurança da informação. Relativamente à perceção do âmbito da ciberdefesa, nomeadamente das lideranças das FA, constata-se estarem ainda iminentemente centradas no conceito *information assurance*, afigurando-se, também aqui, a necessidade de desenvolver programas de sensibilização interna que potenciem a perceção da ciberdefesa como uma capacidade militar que concorre para o conhecimento situacional, proteção e emprego da força. No entanto, é ao nível das dimensões estrutura e organização que são mais visíveis as lacunas das FA. Desde logo porque o CCD, situado ao nível conjunto e na dependência do CEMGFA, está vocacionado primariamente para a resposta a incidentes no ciberespaço, numa filosofia de operação tipo CERT, assegurando a coordenação e o trabalho colaborativo e integrado com os núcleos CIRC dos ramos e do EMGFA, tudo numa ótica de cibersegurança. Apesar das atribuições já detidas no âmbito da condução de OC, o CCD não possui, de modo algum, uma orgânica que lhe permita assumir o ciberespaço como componente de operações, estando impossibilitado de assegurar o exercício do ciberespaço com vantagem competitiva para as FA. Também ao nível tático e enquanto elemento incontornável para a implementação de uma força conjunta integrada, não existem ainda cibercapacidades, nomeadamente as específicas dos ramos. Apesar das iniciativas já ocorridas, parece ainda não haver quaisquer reflexos ao nível da incorporação de pessoal para esta nova dimensão, nem ao nível do pessoal militar nem ao nível do pessoal civil, cuja admissão parece ser inevitável face às condicionantes técnicas e de permanência em funções oportunamente analisadas. Em jeito conclusivo, pode-se afirmar que, apesar do inquestionável esforço desenvolvido pelo EMGFA desde 2015, com inegável sucesso área da ótica da segurança do ciberespaço, o estado atual da ciberdefesa nas FA não configura, ainda, uma capacidade militar, carecendo, para tal, de serem implementados, ou melhor adequados, alguns dos vetores de desenvolvimento.

Por último e de acordo com o OE3, a investigação centrou-se na análise de estudos de caso relativos a sistemas de ciberdefesa já consolidados, procurando elencar contributos nas

dimensões do MA. Foi possível apurar do aspeto dual do ciberespaço – promotor de progresso e bem-estar, mas também de conflitualidade – cujos objetivos se vêm deslocando da esfera da informação para objetivos mais tangíveis, crescentemente associados às IC e serviços essenciais dos países e organizações. No âmbito estritamente militar e nos estudos de caso considerados, foi também possível identificar os esforços conducentes à estratificação do ciberespaço, à sistematização do espectro de OC, à edificação de uma estrutura de ciberdefesa assente num comando de componente, à reformulação dos EM por incorporação de valências de ciberdefesa nas células J6/G6 e à criação de equipas táticas de ciberdefesa, incorporando as especificidades dos ramos e constituindo um todo coerente enquanto força conjunta de ciberdefesa.

Ao nível das pessoas, dimensão considerada em todo o estudo como a mais crítica, foi também possível apurar que a dinâmica e a complexidade do ciberespaço exigem uma adaptação contínua à envolvente operacional, colocando às FA o desafio adicional de recrutar e reter o pessoal mais qualificado, capaz de integrar os requisitos inicialmente estabelecidos e, proativamente, promover a inovação e a evolução constante, tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades.

Como corolário do estudo e em jeito de avaliação de resultados, pudemos verificar que: as FA não estão capazes de conduzir operações no ciberespaço e, como tal, de este ser assumido como domínio operacional; a ciberdefesa não configura ainda uma capacidade militar; da análise a sistemas de ciberdefesa, foram identificados contributos importantes nas dimensões críticas da segurança do ciberespaço. Na linha metodológica adotada, resultam assim validadas as hipóteses de investigação e atingidos os OE propostos, entendendo-se coerente, como resposta à QC da investigação, afirmar que, mantendo os pressupostos da confidencialidade, disponibilidade e integridade da informação dos sistemas de informação, foram identificados contributos para a edificação de uma capacidade de ciberdefesa que assegure a atuação eficaz das FA no ciberespaço.

Contributos para o conhecimento

Os complexos desafios de segurança no ciberespaço que se vêm colocando às FA, firmados também por Portugal no recente reconhecimento do ciberespaço como domínio operacional, alvitram a necessidade de fazer evoluir o atual processo de implementação da ciberdefesa, assumindo-a em todas as vertentes que conceptualmente qualificam uma capacidade militar.

Desde logo, impende delinear um plano estratégico que, nas dimensões operacional e genética, determine o enquadramento doutrinário, a edificação de estruturas e a implementação de processos que capacitem as FA a desempenhar as suas missões nesta nova dimensão, cumprindo o desiderato de instrumento privilegiado de projeção de força da nação, através do exercício de uma presença permanente e vigilante e da capacidade de executar todo o espectro de operações no espaço cibernético.

A capacidade de ciberdefesa deverá envolver o conhecimento e os recursos necessários para prever, influenciar ou bloquear as ações que potenciais adversários venham a desenvolver no ciberespaço, antes e durante as operações militares, e, no contexto da preparação do AO, avaliar o espectro da ameaça e contribuir para a identificação de potenciais agressores garantindo, em tempo, uma resposta eficaz e dissuasora. Numa lógica supletiva de reforço dos aspetos apresentados, esboçam-se, no apêndice E, singelos contributos para o conhecimento, que, numa perspetiva pragmática, poderão eventualmente concorrer para a edificação da capacidade de ciberdefesa, abordando os seguintes tópicos:

- Conceito de ciberdefesa;
- Estratificação do ciberespaço;
- Sistematização do espectro de operações e das ações no ciberespaço;
- Organização da ciberdefesa, nomeadamente apresentando alguns elementos de informação relativos à criação de um órgão que, em complemento da missão de resposta a ciberincidentes, tenha também a capacidade de conduzir operações militares no ciberespaço, assumindo as responsabilidades de comando da componente de ciberdefesa;
- Um ensaio, preconizado em função do MA, sobre TTP de ciberdefesa.

Recomendações e outras considerações de ordem prática

Ao longo do trabalho foram identificados processos e áreas de estudo que suscitam posterior desenvolvimento, merecendo especial destaque os aspetos que se relacionam com o enquadramento e a operacionalização da capacidade de ciberdefesa, sugerindo-se:

- Rever, nos aspetos oportunamente identificados, o CEM e a ENSC.
- Elaborar um plano estratégico para a edificação da capacidade de ciberdefesa considerando duas linhas de ação estratégica principais: garantir a liberdade de ação das FA e de Portugal no ciberespaço; assegurar a capacidade de projetar força no, ou através do, ciberespaço.

Limitações da investigação e abertura para pesquisas futuras

Como principais limitações ao exercício da investigação, identificam-se a inexistência de referências nacionais ao nível da doutrina e do emprego de meios de ciberdefesa e, ao nível dos estudos de caso, a extrema dificuldade de obtenção de informação acionável, mesmo entre países com acordos de partilha de informação de ciberdefesa.

Como epílogo, uma última reflexão: Portugal não pode considerar-se imune aos riscos e ameaças veiculados pelo ciberespaço, com base numa hipotética premissa de se constituir, pelo seu impacto geopolítico, um *soft target*. Seria no mínimo abracadabrante que as FA não se preparassem para fazer face a esta dimensão da conflitualidade e sobretudo que não procedessem às inevitáveis reformas nas dimensões pessoas, processos, tecnologia e estruturas, garantindo, no devir, a adequação das capacidades ao exercício da soberania e independência nacionais.

A implementação da componente de ciberdefesa, considerando os custos reduzidos no universo das capacidades, pode significar o tradicional afastamento da fatalidade financeira como fator limitador à edificação de uma capacidade militar completa, podendo significar uma aposta ganhadora das FA e a afirmação de responsabilidade e autoridade de Portugal neste novo domínio operacional.

Bibliografia

Ackerman, R. K., 2015a. Destructive Cyber Attacks Increase in Frequency, Sophistication. *Signal*, July.

Ackerman, R. K., 2015b. Convergence Dominates Army Cyber Activities. *Signal*, October, pp. 39-41.

Ackerman, R. K., 2015c. Joint Force Headquarters Changes Defense networking. *Signal*, May, pp. 19-21.

Ackerman, R. K., 2015d. Commercial Cyber Vulnerabilities:. *Signal*, May, pp. 28-30.

AFCEA, 2016a. DHS Expands Cyber Work Force. *Signal,* December.p. 9.

AFCEA, 2016b. Millennials May Present Insider Cyberthreat. *Signal,* December.p. 9.

Albright, D., Brannan, P. e Walrond, C., 2016. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*. [Em linha] Disponível em: David Albright, Paul Brannan, and Christina Walrond (2010). "Did Stuxnet Take Out 1,000 Centrifuges at the Nahttp://isis-Em linha.org/uploads/isisreports/doc [Acedido em 2016 outubro 02].

Andrade, A. R., Roseira, C. e Barreto, A. A., 2016. *Informação e ambientes organizacionais.* [Em linha] Disponível em: http://revista.ibict.br/fiinf/article/view/1771/1974 [Acedido em 28 outubro 2016].

AR, 2009. Aprova a Lei Orgânica de Bases da Organização das Forças Armadas (Lei Orgânica nº 1-A/2009). *Diário da República*.

ARCYBERCOM, 2013. *The Next Battlefield (Conferência).* s.l., US Army Cyber Command.

Armée de l'Air, 2015. *Réflexions sur le cyber: quels enjeux?*. s.l.:Ministére de la Defense.

Babcock, C., 2015. Preparing for the Cyber Battleground of the Future. *Air & Space Power Journal, 29(6),* pp. 61-73..

Barber, D. . E., Bobo, A. e Sturm, K. P., 2015. Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains. *Military Cyber Affairs*, Volume Military Cyber Affairs: Vol. 1 : Iss. 1 , Article 3.

Berry, N. e Prugh, W., 2015. Cyber Data analysis Requires Multidimensional Approach. *Signal*, October, pp. 49-50.

Boutherin, G., 2017. Le combat multidomaine. *Défense & Sécurité Internationale*, Janvier-Février, pp. 64-69.

Brandes, S., 2013. The Newest Warfighting Domain: Cyberspace. *Synesis: A Journal of Science, Technology, Ethics, and Policy Volume 4*, Volume 4, pp. G90-95.

Brotby, W. K. e Hinson, G., 2013. *Pragmatic Security Metrics: Applying Metametrics to Information Security.* London; New York: Auerbach Publications.

Bundesamt fuer Sicherheit in der Informationstechnik, 2016. *Die Lage der IT-Sicherheit in Deutschland 2014.* [Em linha] Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht20 [Acedido em 02 novembro 2016].

Camelo, L. F., 2016a. *Cyberspace Strategies - CYS 6326.* Washington D.C.: National Defense University.

Camelo, L. F., 2016b. *Cyber Intelligence - CYI 6232.* Washington D.C.: National Defense University.

Camelo, L., Honorato, M. e Mateus, R., 2017. *O ciberespaço como domínio operacional: impacto estratégico na política de defesa nacional (TIG AEE CPOG 2016/2017).* Lisboa: IUM.

Caton, J. L., 2015. *Army Support of Military Cyberspace Operations: joint contexts and global.* s.l.:The United States Army War CollegeU.

Caudle, D., 2013. *Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context Into Poliheuristic Decision Theory.* [Em linha] Disponível em: https://www.researchgate.net/publication/269709565_Improving_Cyber_Warfare_DecisionMaking_by_Incorporating_Leadership_Styles_and_Situational_Context_into_Poliheuristic_Decision_Theory [Acedido em 03 março 2016].

CCEM, 2014. *Conceito Estratégico Militar.* s.l.:Conselho de Chefes de Estado-Maior.

Chezem, J., 2015. Air Force Cyber Mission Success Depends on Culture Change. *Signal*, October, pp. 42-45.

CNCS, 2017. *Estratégia Nacional de Segurança do Ciberespaço* [Entrevista] (13 janeiro 2017).

ComDCiber, 2016. *Questionário "Estrutura de defesa cibernética no Brasil".* Brasília: Comando de Defesa Cibernética.

Conti, G. N. J. e. R. D., 2013. *Towards a Cyber Common Operating Picture.* Tallin, NATO CCD COE.

Cordell, C., 2016. *Atkin: Cybersecurity, critical infrastructure will be challenges for Trump's DHS.* [Em linha] Disponível em: http://www.federaltimes.com/articles/atkin-cybersecurity-critical-infrastructure-will-be-challenges-for-trump-dhs?utm_source=

Sailthru&utm_medium=email&utm_campaign=Early%20Bird%20Brief%2012.6.2016&utm_term=Editorial%20-%20Early%20Bird%20Brief [Acedido em 05 dezembro 2016].

Couto, A. C., 1988. *Elementos de estratégia, apontamentos para um curso.* Lisboa: IAEM.

CSDN, 2014. *Missões das Forças Armadas MIFA 2014 (CSDN de 30 de julho).* Lisboa: Conselho Superior de Defesa Nacional.

Cunha, F. M. d. M. P., 2017. *Capacidade de ciberdefesa e operações no ciberespaço* [Entrevista] (12 janeiro 2017).

Cutchins, C., 2015. *Engaging Millennials: The Military Way.* [Em linha] Disponível em: http://www.franklinstreet.com/engaging-millennials-the-military-way [Acedido em 19 março 2016].

David, J., 2016. *How Do Cyber Operations Look in 2025?.* [Em linha] Disponível em: http://www.cyberdefensereview.org/ [Acedido em 21 fevereiro 2017].

Davies, K., 2016. Defending Industrial Control Systems From Cyber Attacks. *Signal*, October, pp. 45-46.

Denning, D. E., 2015. Rethinking the Cyber Domain and Deterrence. *JFQ77*, 2nd Quarter, pp. 8-15.

DHS, 2011. *The Strategic National Risk Assessment.* Washington: Office of Risk Management and Analysis, Department of Homeland Security.

Donaldson, P., 2016. Electronic Warfare Solutions. *C4I Forum*, pp. 58-61.

EMGFA, 2012. *PDMC-01 Doutrina Militar Conjunta.* Lisboa: EMGFA.

EMGFA, 2014. *Plano para a edificação da capacidade de ciberdefesa nacional (Ofício n.º 132-CG, de 14JAN14 do EMGFA),* Lisboa: Estado-Maior-General das Forças Armadas.

ENISA, 2012. *National Cybersecurity Strategies: Practical Guide on Development and Execution.,* s.l.: s.n.

Exército Brasileiro, 2013. Defesa Cibernética. *Verde-Oliva,* junho, Volume 217, pp. 28-33.

Exército, 2012. *PDE 3-00 Operações.* Lisboa: Exército.

Exército, 2014. *PDE 3-01-00 Tática das Operações de Combate Volume 1 1º Draft.* Lisboa: Estado-Maior do Exército.

Exército, 2015. *Normas de Gestão de Projetos do Exército.* Lisboa: Divisão de Planeamento de Forças do Estado-Maior do Exército.

Fahrenkrug, D. T., 2007. *Cyberspace Defined.* [Em linha] Disponível em: http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm [Acedido em 29 outubro 2016].

Felício, J. A. d. J., 2008. *Planeamento Estratégico: Actividade funcional estruturada.* Lisboa, ISEG.

Franz, T., 2011. The Cyber Warfare Professional: Realizations for Developing the Next Generation. *Air & Space Power Journal: Realizations for Developing the Next Generation*, pp. 87-99.

GAO, 2004. *Combating Terrorism Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* Washington, D.C. 20548: General Accounting Office.

GAO, 2010. *US Faces challenges in addressing global cybersecurity and governance,* Washington, D.C. 20548: General Accounting Office.

GAO, 2011. *DoD Faces Challenges In Its Cyber Activities,* Washington, D.C. 20548: General Accounting Office.

Giandomenico, A., 2015. Threat Research the Secretsof Cyber Hazards. *Signal*, October, pp. 46-48.

Gobierno de España, 2013. *Estrategia de Ciberseguridad Nacional.* [Em linha] Disponível em: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional [Acedido em 28 março 2017].

González, A., 2017. Stoltenberg advierte de que un ciberataque activaría la defensa común en la OTAN. *El País*, 20 janeiro.

Governo do Brasil, 2014. *Diário Oficial da União.* [Em linha] Disponível em:http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/10/2014&jornal=1&pagina=7&totalArquivos=56 [Acedido em 27 outubro 2016].

Governo, 2013a. Conceito Estratégico de Defesa Nacional (Resolução do Conselho de Ministros n.º 19/2013). *Diário da República*, 5 abril, pp. 1981-1995.

Governo, 2013b. Defesa 2020 (Resolução do Conselho de Ministros n.º 26/2013). *Diário da República*, 11 abril.

Governo, 2014a. Aprova a estrutura orgânica da Marinha (Decreto-Lei nº185/2014 de 29 de dezembro). *Diário da República*, 29 dezembro.

Governo, 2014b. Aprova a orgânica do MDN (Decreto-Lei n.º 183/2014 de 29 de dezembro). *Diário da República*, 29 dezembro.

Governo, 2014c. Aprova a estrutura orgânica do Exército (Decreto-Lei nº 186/2014 de 29 de dezembro). *Diário da República*, 29 dezembro.

Governo, 2014d. Lei orgânica do EMGFA (Decreto-Lei n.º 184/2014, de 29 de dezembro). *Diário da República*, 29 dezembro.

Governo, 2014e. Aprova a estrutura orgânica da Força Aérea (Decreto-Lei nº 187/2014 de 29 de dezembro). *Diário da República*, 29 dezembro.

Governo, 2015a. Aprova a orgânica da Força Aérea (Decreto Regulamentar nº12/2015 de 31 de julho). *Diário da República*.

Governo, 2015b. Orgânica Interna do EMGFA (Decreto Regulamentar nº13/2015 de 31 de julho). *Diário da República*, 31 julho, pp. 5275-5295.

Governo, 2015c. Aprova a orgânica do Exército (Decreto Regulamentar nº11/2015 de 31 de julho). *Diário da República*, 31 julho.

Governo, 2015d. Aprova a orgânica do EMGFA (Decreto Regulamentar nº13/2015 de 31 de julho). *Diário da República*, 31 julho, pp. 5275-5295.

Governo, 2015e. Aprova a orgânica da Marinha (Decreto Regulamentar nº10/2015 de 31 de julho). *Diário da República*, 31 julho.

Governo, 2015f. Estratégia Nacional de Segurança do Ciberespaço (Resolução do Conselho de Ministros n.º 36/2015, de 28 de maio). *Diário da República, 1ª série - N.º113*, 12 junho, pp. 3738-3742.

Gutman, Y., 2016. *The Objective: Operational Cyber Intelligence.* [Em linha] Disponível em: http://www.israeldefense.co.il/en/content/objective-operational-cyber-intelligence [Acedido em 5 outubro 2016].

Harris, R., 2016. Army Braces for a Culture Clash. *Signal*, January, pp. 36-38.

Hedstrom, M. A., 2001. *Simultaneity: A Question of Time, Space, Resources and Purpose.* Fort Leavenworth: School of Advanced Military Studies.

IATAC, 2009. *Vulnerability Assessment, Defense Technical Info Centre,* s.l.: s.n.

IDN, 2013a. *Conceito Estratégico de Defesa Nacional 2013 Contributos e Debate Público.* Lisboa: Instituto da Defesa Nacional.

IDN, 2013b. *Estratégia da Informação e Segurança no Ciberespaço.* Lisboa: Instituto da Defesa Nacional.

IESM, 2014. *Identificação dos domínios, áreas e subáreas de investigação do IESM (Anexo B à NEP ACA-010-B).* Pedrouços: Instituto de Estudos Superiores Militares.

IESM, 2015a. *Trabalhos de Investigação (NEP ACA - 010).* Pedrouços: Instituto de Estudos Superiores Militares.

IESM, 2015b. *Regras de apresentação e referenciação (NEP ACA 018).* Pedrouços: Instituto de Estudos Superiores Militares.

IISS, 2015. *Evolution of the cyber domain: The implications for national and global security.* London: The International Institute for Strategic Studies.

INSA, 2014. Strategic Cyber Intelligence. March.

IUM, 2016. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação.* Pedrouços: Fronteira do Caos Editores.

Janczewski, L. J. e Colarik, A. M., 2008. *The U.S. Military Response to Cyber Warfare.* New York: s.n.

Jones, J. R. e Averbeck, R., 2015. *The 3 Types of Insider Threat.* [Em linha] Disponível em: http://preemploymentdirectory.com/the-3-types-of-insider-threat/#axzz4MzZWUP6V [Acedido em 13 outubro 2016].

Jontz, S., 2015a. Critical Infrastructure Is Cyberterrorism's Next likely Target. *Signal*, pp. 18-21.

Jontz, S., 2015b. Cybersecurity Education Receives a Makeover. *Signal*, April, pp. 35-37.

Jontz, S., 2016a. Taking Cyber War to the Front Lines. *Signal*, October, pp. 20-23.

Jontz, S., 2016b. U.S. Army Creates Cybersecurity strategy For a New Normal. *Signal*, October, pp. 35-38.

Jontz, S., 2016c. Cyber Ethics Vex online Warfighters. *Signal*, January, pp. 32-34.

Jontz, S., 2016d. Wining Wars at the Speed of Cyber, Not Acquisition Cycles. *Signal*, December, p. 40.

kenkov, V. e Naumovski, T., 2014. *Concept and priorities of cyber defence.* [Em linha] Disponível em:http://eds.b.ebscohost.com.nduezproxy.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=1&sid=7066beb7-8df0-45b4-91fe-4cdb269197e%40sessionmgr105&hid=104 [Acedido em 05 dezembro 2016].

Kern, S., 2015. Expanding Combat Power Through Military Cyber Power Theory. *Joint Force Quarterly (79)*, pp. 88-95.

Kreisher, O., 2016. The Future Fight. *Seapower*, March, pp. 14-17.

Kshetri, N., 2014. Kshetri, N 2014, 'Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses', , 31, 3, p. 183, Publisher. *East Asia: An International Quarterly*, March, pp. 183-201.

Kshetri, N., 2016. The Quest to Cyber Superiority. Em: *The Quest to Cyber Superiority.* s.l.:s.n.

Lee, S.-k. e Kang, T.-i., 2015. Adaptive Multi-Layer Security Approach for Cyber Defense. *Journal of Internet Computing and Services,* pp. 01-09.

Loerch, J., 2016. What We Have Is a Failure to Communicate. *Signal*, February, pp. 29-31.

Lopes, J. A. d. A. F., 2016. *Intervenção do Ministro da Defesa Nacional na conferência A Cimeira da NATO em Varsóvia e o novo ambiente de segurança internacional.* Lisboa, Gabinete do Ministro da Defesa Nacional, p. 12.

M., M. e A., A., 2017. *Dilemma Transformation 5 Generation.* 127 ed. s.l.:Défense & Sécurité Internationale.

Marques, A. G., 2017a. *Capacidade de ciberdefesa e operações no ciberespaço* [Entrevista] (19 janeiro 2017a).

Marques, A. G., 2017b. *O Poder da Informação no Poder Militar (Conferência ao CPOG 2016-2017, em 2017-02-21).* Lisboa, IUM.

MCCD, 2016a. *Estructura de Ciberdefensa en España [Questionário]*. Madrid: Mando Conjunto de Ciberdefensa.

MCCD, 2016b. *National Strategic and Operational vision of Cyber Operations [Conferência]*. Lisboa, IUM.

MDN, 2013. Orientação política para a ciberdefesa (Despacho n.º 13692/2013). *Diário da República, 2ª série - N.º 208*, 28 outubro, pp. 31977-31979.

MDN, 2014a. Diretiva Ministerial de Planeamento de Defesa Militar (Despacho n.º 11400/2014). *Diário da República, 2.ª série — N.º 175*, 11 setembro, pp. 23656-23657.

MDN, 2014b. *Plano para a edificação da capacidade de ciberdefesa nacional (Desp. n.º 33/2014).* Lisboa: Ministério da Defesa nacional.

MDN, 2014c. *Sistema de Forças 2014.* Lisboa: MDN.

Metz, S. e Kievit, J., 1995. *Strategy and the Revolution in Military Affairs.* s.l.:US Army.

Ministério da Defesa do Brasil, 2014. *Doutrina Militar de Defesa Cibernética (MD31-M-07).* Brasília: Estado-Maior Conjunto das Forças Armadas.

Ministerio de Defensa, 2014. El Mando Conjunto de Ciberdefensa Art.º 15 do Real Decreto 872/2014. *Boletín Oficial del Estado*, 10 octubre, pp. 84086-84100.

MITRE, 2014. *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford, MA: s.n.

Monteiro, A. P., 2017. *Capacidade de ciberdefesa e operações no ciberespaço* [Entrevista] (02 fevereiro 2017).

Moreira, A., 2017. *Portugal e a ONU.* Lisboa, IUM.

NATO, 2014a. *Enhanced NATO Policy on Cyber Defence (PO2014/0358), 27 May,* Brussels: NATO.

NATO, 2014b. *NATO Cyber Defence Taxonomy and Definitions.* Norfolk: NATO Consultation, Command and Control Board.

NATO, 2015a. *Assessment of target ambition levels for CIS security (AC/322-N2015/0033).* Brussels: s.n.

NATO, 2015b. *Food for Thought Paper on the Cyber Dimension of Hybrid Warfare,* Brussels: International Staff.

NATO, 2016a. *BI-SC Final assessment of recognising cyberspace as a domain (IMSWM-0190-2016),* Brussels: BI-SC.

NATO, 2016b. *Military advice on the recognition of cyberspace as a domain (MCM-0083-2016),* Brussels: Military Committee.

NATO, 2016c. *Cyber Defence Capability Breakdown (AC/322-D2016/0050),* Brussels: C3B.

NATO, 2016d. *Warsaw Summit Communiqué.* Warsaw, NATO.

NATO, 2016e. *NATO Cyber Defence.* Brussels, Public Diplomacy Division.

NATO, 2017a. *AJP-3.20 Doctrine for Cyberspace Operations.* Version 1 (2017/01/26) ed. Brussels: NATO.

NATO, 2017b. *NATO.* [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/topics_78170.htm [Acedido em 24 março 2017].

Neves, N. C., 2015. Um maior do que Guderian – Tukhachevsky e o desenvolvimento das Forças Armadas Soviéticas. Em: *Revista de Ciências Militares, Vol. III, N.º 1 – Maio de 2015.* s.l.:Instituto de Ensino Superior Militar, pp. 127-158.

Neves, P. J. B., 2015. *Capacidade de resposta incidentes de segurança da informação no ciberespaço.* Lisboa: s.n.

NICCS, 2015. *National Initiative for Cybersecurity Careers and Studies - A Glossary of Common Cybersecurity Terminology,* s.l.: National Initiative for Cybersecurity Careers and Studi.

NIST, 2013a. *800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations,* s.l.: NIST.

NIST, 2013b. *NISTIR 7298 Glossary of Key Information Security Terms,* s.l.: Richard Kissel.

NIST, 2014. *Guide to Cyber Threat Information Sharing.* Washington: NIST.

Nunes, P. V., 2015. *Sociedade em Rede, Ciberespaço e Guerra da Informação. Contributos para o Enquadramnto e Construção de Uma Estratégia Nacional de Informação.* s.l.:Instituto da Defesa Nacional.

Pereira, J., 2013. O ciberespaço e a mutação da realidade: o caso dos EUA. *Instituto da Defesa Nacional*, novembro.

Pires, J., 2016. *Capacidade de ciberdefesa e operações no ciberespaço* [Entrevista] (13 dezembro 2016).

Pires, N. M. V., 2016. *Capacidade de ciberdefesa e operações no ciberespaço* [Entrevista] (16 dezembro 2016).

Pomerleau, M., 2016a. *Cyber mission force reaches key milestone.* [Em linha] Disponível em: http://www.c4isrnet.com/articles/cyber-mission-force-reaches-key-milestone [Acedido em 02 January 2017].

Pomerleau, M., 2016b. *CYBERCOM evaluating cyber mission force.* [Em linha] Disponível em: http://www.c4isrnet.com/articles/cybercom-evaluating-cyber-mission-force?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20EBB%2012.15.16&utm_term=Editorial%20-%20Early%20Bird%20Brief [Acedido em 02 janeiro 2017].

PRBrasil, 2008. Estratégia Nacional de Defesa (Decreto nº 6.703). *Diário Oficial da União*, 18 dezembro.

PRBrasil, 2011. *Desafios estratégicos para a segurança e defesa cibernética.* 1ª ed. Brasília: Secretaria de Assuntos Estratégicos.

Rajnovic, D., 2012. *Cyberspace – What is it?,* San José, Califórnia, EUA: CISCO.

Reilly, J., 2016. Multidomain Operations: A Subtle but Significant Transition in Military Thought. *Air & Space Power,* Volume Spring, pp. 61-73.

Ring, B., Brown, R., Howard, L. e Ness, P., 2014. Leading Structured Organization in the Dynamic Information Age. *Military Review*, March-April.

Ritchey, D., 2014. Cyber Risk and Special Security Report. *Security: Solutions For Enterprise Security Leaders, 51(2)*, pp. 40-46.

Roodt, J., Oosthuizen, R. e Vuuren, J., 2015. *Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces.* s.l., Conference on Information Warfare e Security.

Rumelt, R., 2011. The perils of bad strategy. pp. 30-39.

Russell, A. L., 2017. *Strategic A2/AD in Cyberspace.* 1ª ed. Massachusetts: Merrimack College.

Saïd Business School, 2016. *Cyber Harm: Concepts, Taxonomy and Measurement.* s.l.:Saïd Business School.

Santos, L., 2001. *Segurança e Defesa na Viragem do Milénio: Reflexões sobre Estratégia II.* Mem Martins: Publicações Europa América.

Schwab, K., 2016. Em: *A Quarta Revolução Industrial.* s.l.:s.n., p. 160.

Seffers, G., 2015a. Cyber Is a Global Team Support. *Signal*, March, pp. 26-28.

Seffers, G., 2015b. U.S. Army Builds Cyber Branch One Step at a Time. *Signal*, April, pp. 38-41.

Seffers, G., 2016. Russia Converges Electronic Warfare, Cyber Operations. *Signal*, October, pp. 48-49.

Seffers, G., 2017. Cyber Maximizes Combat Power: Yey the military faces obstacle in integrating cyber with other warfighting realms.. *Signal*, October, p. 34.

SEI, 2013. *Improving Operational Resilience Processes. CERT® Resilience Management Model V1.1.* .. [Em linha] Disponível em: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_68641.pdf [Acedido em 23 março 2016].

SEI, 2014. *CERT Resilience Management Model ,* Hanscom: Carnegie Mellon University.

Simpkin, R. E., 1988. *Race to the Swift: Thoughts on 21st Century Warfare.* London: Brassey's Defence Publishers.

Singer, P. e Friedman, A., 2014. *Cybersecurity and Cyberwar: What everyone needs to know.* Oxford: Oxford University Press.

Slocombe, G., 2016. Offensive Military Cyber Operations. *Asia Pacific Defence Reporter*, november, pp. 26-28.

Sprong, E., 2016. *Dutch Cyber Strategy.* s.l., Ministry of Defence.

Steiner, G. A., 1979. *Strategic Planning.* s.l.:Free Press.

Strassmann, P., 2015. Cyberwarfar Needs More Brains. *Signal*, April, pp. 49-50.

Stytz, M. e Banks, S., 2014. Toward Attaining Cyber Dominance. *Strategic Studies Quarterly*, Spring, pp. 55-87.

Taylor, D. P., 2016. Force Multiplier: Navy looks to develop cyber capabilities as part of its air warfare domain. *Seapower*, October.

The Economist, 2010. *CYBERWAR: It is time for countries to start talking about arms control on the internet.* [Em linha] Disponível em: http://www.economist.com/node/16481504 [Acedido em 10 novembro 2016].

UE, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Brussels: European Union.

UE, 2015. *Cybersecurity and cyberdefence: EU Solidarity and Mutual Defence Clauses.* Brussels: European Union Parliament.

UE, 2016a. *Quadro comum em matéria de luta contra as ameaças híbridas. Uma resposta da União Europeia.* Bruxelas, União Europeia.

UE, 2016b. *Estratégia global para a política externa e de segurança da União Europeia.* Bruxelas: União Europeia.

UE, 2016c. *EU Concept on Cyber Defence for EU-led Military Operations and Missions, Rev 2,* Brussels: União Europeia.

UKCabinet, 2015. *National Risk Register of Civil Emergencies.* London: UK Cabinet Office.

UKMoD, 2015. *Future Operating Environment 2035.* London: Development, Concepts and Doctrine Centre.

US Army, 1996. *FM 100-6 Information Operations.* s.l.:HQ TRADOC.

US Cyber Command, 2015. *Beyond the Build, Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for US Cyber Command,* Fort Meade: Department of Defense.

US Department of Defense, 2016. *JP 1-02 - Dictionary of Military and Associated Terms.* USA: DoD.

US White House, 2011. *International Strategy for Cyberspace.* [Em linha] Disponível em: https://www.whitehouse.gov/sites/default/files/rss_viewer /international_strategy_for_cyberspace.pdf [Acedido em 26 setembro 2016].

USJCS, 2012. *Joint Operational Access Concept.* s.l., Joint Chiefs of Staff United States Armed Forces.

USJCS, 2013. *JP 3-12(R) - Cyberspace Operations,* Washington DC: United States Joint Chiefs of Staff.

USJCS, 2014. *JP 3-13 - Information Operations.* s.l.:United States Joint Chiefs of Staff.

USJCS, 2016. *Cross Domain Synergy in Joint Operations Planner's.* Washington D.C.: Joint Chiefs of Staff United States Armed Forces.

Veiga, R. d. Q., 2012. *Defesa cibernética na visão da Força Aérea Brasileira.* [Em linha] Disponível em: http://www.portal.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/download/215/18 [Acedido em 27 outubro 2016].

Vicêncio, J. M. d. S., 2016. *Capacidade de ciberdefesa e operações no ciberespaço (Guião 2)* [Entrevista] (03 novembro 2016).

Waddell, D., 2015. *(ISC) Blog: Inspiring a safe and secure cyber world.* [Em linha] Disponível em: http://blog.isc2.org/isc2_blog/2015/05/us-department-of-defense-cyber-strategy-one-of-five-strategic-goals-to-building-and-maintaining-the-.html [Acedido em 14 dezembro 2016].

WeAreSocial, 2017. *Digital in 2017: Global Overview.* [Em linha] Disponível em: https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview [Acedido em 26 abril 2017].

Westphal, M., 2015d. Building a Capability Development Work Force For the Cyber Age. *Signal*, July, pp. 44-46.

Williams, B. L., 2013. *Information Security Policy Development for Compliance.* s.l.:AUERBACH.

Wilson, C., 2007. *Information operation, electronic warfare, and cyberwar: capabilities and related policy,* Washington D.C.: US CRS Report Congress.

Winston, B. e Patterson, K., s.d. *An Integrative Definition of Leadership.* [Em linha] Disponível em: https://www.regent.edu/acad/global/publications/ijls/new/vol1iss2/winston_patterson.doc/winston_patterson.htm [Acedido em 04 dezembro 2016].

Young-ju, L., 2016. Establishment of a Feasible Cyber Organization Structure to Enhance the Capabilities of Cyberspace Operations in the ROK's Defense Forces. *The Korean Journal of Defense Analysis*, 2 June, pp. 223-248.

Apêndice A — Corpo de conceitos

1. Ambiente Operacional

É entendido como o conjunto de condições, circunstâncias e fatores influenciadores que afetam o emprego de forças militares e influenciam as decisões.

(Exército, 2012, p. 17)

2. Ameaça

É qualquer acontecimento ou ação que contraria a consecução de um objetivo e que normalmente é causador de danos materiais ou morais.

(Couto, 1988, p. 329)

3. Ameaças híbridas

São a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada.

(UE, 2016a, p. 2)

4. *Anti Access* (A2)

Conjunto de ações e capacidades, normalmente de longo alcance, que visam impedir a força adversária de entrar na área operacional.

(USJCS, 2012)

5. *Area Denial* (AD)

Conjunto de ações e capacidades, normalmente de curto alcance, que não negando o acesso à força adversária, visam limitar sua liberdade de ação dentro da área operacional.

(USJCS, 2012)

6. Áreas de capacidades

São de natureza conjunta entendidas nos seus efeitos operacionais, se deverá enquadrar a capacidade de ciberdefesa. O CEM estabelece as seguintes: Comando e Controlo; Emprego da Força; Proteção e Sobrevivência; Mobilidade e Projeção; Conhecimento Situacional; Sustentação; Autoridade, Responsabilidade, Apoio e Cooperação.

(CCEM, 2014, p. 17)

7. Capacidade militar

Conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade.

(MDN, 2014a, p. 23657)

8. Ciberataque

Ato ou ação iniciada no ciberespaço para causar dano através do compromisso das comunicações da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas.

(NATO, 2014b)

9. Ciberespaço

Um domínio global e virtual criado pela interligação de todas as redes de comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas.

(NATO, 2014b)

10. Ciberdefesa

A aplicação das medidas de segurança para proteger os componentes da infraestrutura TIC contra ciberataques, sendo estes ciberataques assumidos como uma forma de guerra cibernética, que pode ocorrer em combinação com um ataque físico ou não, que se destina a perturbar os sistemas de informação de um adversário.

(IDN, 2013b, p. 11)

Os meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações, da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas.

(NATO, 2014b)

É uma dimensão da cibersegurança (principalmente vista como sendo a dimensão militar, mas englobando as vertentes tanto militares como civis). Pode ser considerada como as medidas para defender os sistemas críticos e a informação de modo a garantir a cibersegurança.

A Ciberdefesa compreende todas as medidas técnicas e não técnicas para melhorar a resiliência das comunicações e sistemas de informação de apoio aos sistemas de defesa dos estados membros e da sua segurança nacional, bem como as ações conducentes à prevenção, deteção, reação e recuperação de ciberataques a esses sistemas.

(UE, 2016c)

11. Cibersegurança:

Estratégia, política e normas com vista à segurança das operações no ciberespaço, abrangendo missões de redução da ameaça, de vulnerabilidades, de compromisso internacional, de resposta a incidentes, resiliência, e políticas de recuperação, incluído operações em rede, garantia da informação, ações judiciais, diplomáticas, militares e de informações relacionadas com a segurança e estabilidade da infraestrutura global de informação e comunicações.

(NICCS, 2015)

12. Cross-Domain Synergy

O emprego de capacidades em diferentes domínios operacionais, no pressuposto de que cada um deles aumenta a eficácia e minimiza as vulnerabilidades dos outros, assegurando a superioridade a liberdade de ação necessária ao sucesso da missão.

(USJCS, 2012)

13. Domínio

A esfera de interesse e influência em que as atividades, funções e operações são realizadas de modo a cumprir missões e exercer o controlo sobre um adversário, a fim de se obterem os desejados.

(NATO, 2016a, p. 5)

14. Evento

Uma ocorrência num sistema, serviço ou rede indicando uma possível quebra de segurança da informação, política ou falha de controlos, ou uma situação desconhecida que poderá ser significativa em termos de segurança.

(NIST N. I., 2013)

15. Guerra da Informação

As ações desenvolvidas para obter a superioridade de informação, afetando a informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores de um adversário enquanto se defendem a nossa informação, sistemas de informação e redes baseadas em computadores.

(US Army, 1996, pp. 2-2)

16. Incidente

Uma ocorrência que coloca em risco a confidencialidade, integridade ou a disponibilidade dum Sistema de Informação ou dos seus processos, armazenamento ou transmissão, ou que constitua uma violação ou ameace vir a violar das políticas de segurança, procedimentos de segurança ou políticas em vigor.

(NIST, 2013a, p. B9)

Apêndice B — Lista de entidades

Entidade	Cargo	Data Local	Guião
Gen Pina Monteiro	Chefe do Estado-Maior-General das Forças Armadas	02/02/2017 EMGFA Lisboa	Guião 1 Tabela 8 e 9
VAlm Fernando Cunha	Chefe do Estado-Maior do Comando Conjunto para as Operações Militares	12/01/2017 CCOM Oeiras	Guião 1 Tabela 8 e 9
Cmdr Jorge Pires	Diretor de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas	13/12/2016 EMGFA Lisboa	Guião 2 Tabela 8 e 9
MGen Viegas Pires	Diretor de Comunicações e Sistemas de Informação do Exército	16/12/2016 DCSI Lisboa	Guião 2 Tabela 8 e 9
MGen José Vicêncio	Diretor de Comunicações e Sistemas de Informação da Força Aérea.	03/11/2016 EMFA Amadora	Guião 2 Tabela 8 e 9
CAlm Gameiro Marques	Diretor-Geral do Gabinete Nacional de Segurança e anterior Superintendente das Tecnologias de Informação da Marinha	19/01/2017 GNS Lisboa	Guião 2 Tabela 8 e 9
Cor Luís Camelo	Chefe do CCD (Universo Forças Armadas e Exército)	04/11/2016 CCD Lisboa	Tabela 8 e 9
CTen Francisco Assunção	Adjunto do chefe do Centro de Ciberdefesa (Universo Forças Armadas e Marinha)	14/03/2017 CCD Lisboa	Tabela 8 e 9
Maj João Farinha	Adjunto do chefe do Centro de Ciberdefesa (Universo Forças Armadas e Força Aérea)	14/03/2017 CCD Lisboa	Tabela 8 e 9

Apêndice C — Guião das entrevistas

I

CAPACIDADE DE CIBERDEFESA E OPERAÇÕES NO CIBERESPAÇO
1. O ciberespaço foi considerado um novo domínio operacional. Qual o impacto para as Forças Armadas (organizacional, estrutural, doutrinário, infraestruturas, operações, outros)?
2. Que estrutura para a ciberdefesa nas Forças Armadas?
3. Principais cenários, desafios e ameaças à segurança e defesa do ciberespaço.
4. Qual o nível de ameaça no/através do ciberespaço considerado inaceitável para as FA (acima do qual se exige uma postura ofensiva)?
5. Qual o conceito de operações (CONOPS) no ciberespaço? Como integrar o planeamento e a execução das operações no ciberespaço com as restantes operações militares?
6. Existem programas orientados para preparação das chefias e estados-maiores para este novo ambiente operacional?
7. Considerando a dinâmica elevada de processos e interações que ocorrem no ciberespaço, avaliar da necessidade de se implementar um processo de tomada da decisão específico para as ações de resposta no ciberespaço?
8. A estrutura de ciberdefesa cibernética tem ou deverá ter operadores civis? Em caso afirmativo a que nível organizacional devem estar colocados? Quais as competências e atribuições principais?
9. Outros aspetos considerados pertinentes.

II

CAPACIDADE DE CIBERDEFESA E OPERAÇÕES NO CIBERESPAÇO	
1.	Articulação entre ciberdefesa e a segurança das comunicações e sistemas de informação.
2.	Como visualizam a estrutura da ciberdefesa nas Forças Armadas?
3.	Principais cenários, desafios e ameaças à segurança e defesa do ciberespaço.
4.	Considerando a dinâmica elevada de processos e interações que ocorrem no ciberespaço existe um processo de tomada da decisão específico para as ações de resposta no ciberespaço?
5.	Num incidente cibernético grave, como visualizam a ação de um eventual Comando de Ciberdefesa (nível conjunto) num dos ramos das Forças Armadas. A intervenção seria direta (imediata) ou necessitaria de seguir o habitual procedimento/autorização do ramo? Como compatibilizar o tempo de intervenção em face da dinâmica de processos no ciberespaço?
6.	Existe uma avaliação das capacidades existentes e das vulnerabilidades?
7.	O ciberespaço foi considerado um novo domínio operacional. Qual o impacto para a organização (estrutural, doutrinário, infraestruturas, operações,....)?
8.	Qual o nível de ameaça no/através do ciberespaço considerado inaceitável para a organização (acima do qual se exige uma postura ofensiva)?
9.	Qual o conceito de operações (CONOPS) no ciberespaço? Como integram o planeamento e a execução das operações no ciberespaço com as restantes operações militares?
10.	Existe formação na área da ciberdefesa? Existe alguma estrutura ou órgão com a missão específica de ministrar formação nesta área?
11.	Existem programas orientados para preparação das chefias e estados-maiores para este novo ambiente operacional?
12.	A admissão (de base) do pessoal para ciberdefesa deverá ser diferenciada, obedecendo a requisitos específicos?
13.	As novas gerações estão especialmente habilitadas para trabalhar no ciberespaço. Em contraponto, constata-se a dificuldades em trabalharem e operarem em organizações e estruturas com uma forte componente hierárquica, como é o caso das Forças Armadas. Quais as respostas a estes desafios? Novos modelos de incorporação?
14.	A estrutura de ciberdefesa cibernética tem ou deverá ter operadores civis? Em caso afirmativo a que nível organizacional devem estar colocados? Quais as competências e atribuições principais?
15.	Definição, conceito ou entendimento de ciberespaço e de ciberdefesa.
16.	Existe uma doutrina de ciberdefesa (ou segurança do ciberespaço)?
17.	Quais as principais linhas de ação estratégica?
18.	Que capacidades operativas devem integrar a defesa do ciberespaço?
19.	A área da ciberdefesa tem um orçamento específico? Quem é a entidade responsável pela gestão?
20.	Outros aspetos considerados pertinentes.

Apêndice D — Guião dos questionários

ESTRUTURA DE DEFESA CIBERNÉTICA NO BRASIL

1. CONSIDERAÇÕES GERAIS

As seguintes questão visam essencialmente recolher informação, de natureza não classificada e que na maioria das vezes está publicada, relativamente à estrutura de ciberdefesa dos países pertencentes ao foro iberoamericano, com o objetivo de melhor se poder perspetivar o levantamento completo desta capacidade. Para o efeito solicita-se respostas às questões enunciadas bem como o envio dos respetivos documentos e organogramas das estruturas que estão por base.

2. CONCEITOS E DOUTRINA

Relativamente ao quadro legal e doutrinário para levantamento da capacidade de ciberdefesa

2.1. Definições e conceitos utilizados ou adotados

- 2.1.1. Ciberespaço ou espaço cibernético
- 2.1.2. Segurança cibernética
- 2.1.3. Defesa cibernética
- 2.1.4. Quais são os órgãos com responsabilidades e missões na segurança cibernética e na defesa cibernética?
- 2.1.5. Como e quem faz a articulação entre segurança e defesa cibernética?

2.2. Segurança do ciberespaço

- 2.2.1. Qual é o documento enquadrante (que tutela) as questões da segurança do ciberespaço?
- 2.2.2. Existe uma estratégia nacional de segurança do ciberespaço?
- 2.2.3. Qual é o órgão responsável pela segurança do ciberespaço?
- 2.2.4. Domínio e competências da segurança cibernética.

2.3. Ciberdefesa

- 2.3.1. Existe uma estratégia de defesa cibernética?
- 2.3.2. Quais são as principais linhas de ação estratégica?
- 2.3.3. Domínio e competências da defesa cibernética.
- 2.3.4. Quais são os principais cenários e desafios que se colocam à defesa cibernética?

3. ORGANIZAÇÃO DA ESTRUTURA DA DEFESA CIBERNÉTICA

3.1. Missões de ciberdefesa

3.2. Órgãos e estrutura orgânica de defesa cibernética (decisão, coordenação e estado-maior, execução,..).

3.3. A estrutura da defesa cibernética está inserida no nível conjunto ou nos Exército, Marinha e Aeronáutica?

3.4. A que nível organizacional estão colocados os órgãos de defesa cibernética (estratégico, operacional, tático)?

3.5. O Comando de Defesa Cibernético Brasileiro

3.5.1. Qual a organização (organograma), constituição e missões?

3.5.2. Como se integra com os restantes órgãos de ciberdefesa:

3.5.2.1. De natureza tática (tem órgãos de ciberdefesa de nível tático?);

3.5.2.2. Órgãos do Exército, Marinha e Força Aérea.

3.6. Qual a sua dependência hierárquica e funcional do Comando e da estrutura de defesa cibernética?

3.7. Como se articula a defesa cibernética e a segurança das comunicações e sistemas de informação (CIS) da defesa nacional e das Forças Armadas?

3.8. A ação do Comando de Defesa Cibernética num incidente cibernético no Exército, Marinha ou Aeronáutica é direta ou necessita de prévia autorização cos chefes de estado-maior dos ramos (Exército, Marinha e Aeronáutica)?

4. OPERAÇÕES MILITARES NO CIBERESPAÇO.

4.1. Conceito de Operações (CONOPS) e definição

4.2. Quem é o responsável?

4.3. Como integram o planeamento e execução das operações militares no ciberespaço com as restantes operações militares (nos outros domínios)?

4.4. O ciberespaço vem sendo considerado um novo domínio operacional para as forças armadas. Qual o impacto (organizacional, estrutural, doutrinário, recursos, orçamento, infraestruturas, operações,….) nas Forças Armadas?

5. FORMAÇÃO E TREINO

5.1. Há uma estrutura específica ou uma escola para a formação profissional específica na área da ciberdefesa?

5.2. O treino é conjunto ou é realizado ao nível do Exército, Marinha e Aeronáutica? Há diferenças na formação entre os ramos das Forças Armadas?

5.3. Há uma estrutura funcional de adestramento em ciberdefesa? Qual a dependência?

6. LIDERANÇA

6.1. Existe algum programa especial para preparar as chefias para este novo ambiente operacional?

6.2. Considerando a dinâmica elevada de processos e interações que ocorrem no ciberespaço existe um processo de tomada da decisão específico para as ações de resposta no ciberespaço?

7. PESSOAL

7.1. Nas Forças Armadas existe uma especialidade (quadro de pessoal específico de base) para a defesa cibernética?

7.2. Existe uma carreira militar específica para a ciberdefesa? Caso afirmativo é ao nível conjunto ou dos exércitos?

7.3. A admissão de pessoal para ciberdefesa

7.3.1. É diferenciada?

7.3.2. Tem requisitos próprios?

7.3.3. É feita ao nível conjunto ou nos 3 exércitos? Qual o processo?

7.3.4. As novas gerações (*millennials* ou geração Y) estão especialmente habilitadas para trabalhar no ciberespaço, no entanto têm dificuldades em trabalhar e operar em organizações com uma forte componente hierárquica como é o caso das Forças Armadas. Quais as respostas a estes desafios? Foram implementaram novos modelos de incorporação? Quais?

7.3.5. A estrutura de defesa cibernética tem operadores civis? Em caso afirmativo a que nível organizacional estão colocados? Quais as competências e atribuições/tarefas principais?

8. INFRAESTRUTURAS DA DEFESA CIBERNÉTICA

8.1. Quais são?

8.2. Qual a sua dependência (hierárquica, funcional, logística…).

8.3. Pertencem ao nível conjunto ou dos exércitos?

9. ORÇAMENTO E FINANÇAS

9.1. A estrutura da defesa cibernética tem um orçamento específico?

9.2. Qual é a entidade que gere o orçamento para a defesa cibernética?

ESTRUCTURAS DE CIBERDEFENSA EN ESPAÑA

1. CONSIDERACIONES GENERALES

Las siguientes cuestiones tienen por finalidad obtener información relativa a la estructura de ciberdefensa de los países pertenecientes al foro iberoamericano, de naturaleza no clasificada y que en la mayor parte de los casos se encuentra publicada, al objeto de disponer de una mejor perspectiva para la completa edificación de esta capacidad en Portugal. A tal efecto, se solicita respuesta a las cuestiones referidas a continuación, así como el envío, siempre que sea posible, de los documentos de referencia y los organigramas de las estructuras consideradas.

2. CONCEPTOS Y DOCTRINA

En lo referido al marco legal, conceptual y doctrinal de la capacidad de ciberdefensa

2.1. Definiciones y conceptos[52]

- 2.1.1. Ciberespacio;
- 2.1.2. Ciberseguridad;
- 2.1.3. Ciberdefensa;
- 2.1.4. Órganos y responsabilidades/misiones de la ciberseguridad y ciberdefensa
- 2.1.5. ¿Como se articulan las responsabilidades de estas 2 áreas?

2.2. Seguridad del ciberespacio

- 2.2.1. ¿Cuál es el documento marco (el de mayor nivel, el que tutela) las cuestiones de la seguridad del ciberespacio?
- 2.2.2. ¿Existe una Estrategia Nacional de Seguridad de ciberespacio?
- 2.2.3. ¿Cuál es el órgano responsable de la seguridad del ciberespacio nacional?
- 2.2.4. Dominio y competencias de la ciberseguridad.

2.3. Ciberdefensa

- 2.3.1. ¿Existe una Estrategia de ciberdefensa?
- 2.3.2. ¿Cuáles son las principales líneas de acción estratégica?
- 2.3.3. Dominio e competencias de la ciberdefensa;
- 2.3.4. ¿Cuáles son los principales escenarios y desafíos que afronta la ciberdefensa?

[52] Adoptados y en uso.

3. ORGANIZACIÓN DE LA CIBERDEFENSA

3.1. Misiones de la ciberdefensa.

3.2. Órganos y estructura orgánica de la ciberdefensa (decisión, coordinación y Estado Mayor, ejecución...).

3.3. ¿La ciberdefensa es conjunta o se encuentra a nivel de los ejércitos (tierra, mar y aire)?

3.4. ¿A qué nivel organizacional están situados los órganos de ciberdefensa (estratégico, operacional, táctico)?

3.5. ¿El Mando de Ciberdefensa?

3.6. Como se integra el Mando de Ciberdefensa con los órganos de ciberdefensa:

3.6.1. De naturaleza táctica (¿tiene órganos tácticos de ciberdefensa?);

3.6.2. De cada uno de los ejércitos (tierra, mar y aire; tácticos).

3.7. ¿Cuál es la dependencia jerárquica y funcional de la estructura de ciberdefensa?

3.8. ¿Como se articula la ciberdefensa y la seguridad CIS de las Fuerzas Armadas y de la Defesa Nacional?

3.9. ¿La acción del Mando de Ciberdefensa en un incidente cibernético en los ejércitos es directa o precisa pasar por la autorización del jefe de cada ejército?

4. LAS OPERACIONES MILITARES EN EL CIBERESPACIO.

4.1. Concepto (CONOPS) y definición;

4.2. ¿Quién es el responsable?

4.3. ¿Cómo se integran la planificación y ejecución de operaciones cibernéticas con otras operaciones militares?

4.4. La OTAN y los países miembros han considerado el ciberespacio como el 5º dominio operacional (Cumbre de Varsovia, 2016). ¿Cuál es el impacto en las Fuerzas Armadas?

5. ENTRENAMIENTO Y FORMACIÓN EN CIBERDEFENSA

5.1. ¿Existe alguna especialidad de formación base para la ciberdefensa?

5.2. ¿Hay una estructura específica o una escuela para la formación profesional en ciberdefensa?

5.3. ¿El entrenamiento es conjunto o es realizado a nivel de los ejércitos? ¿Hay diferencias en la formación a nivel de los ejércitos (tierra, mar y aire)?

5.4. ¿Hay una estructura funcional de entrenamiento en ciberdefensa? Si así fuese, ¿de quien depende?

6. LIDERAZGO EN CIBERDEFENSA

6.1. ¿Existe algún programa especial para preparar a los Jefes y Mandos para este nuevo ambiente operacional?

6.2. Considerando la intensa dinámica de procesos e interacciones que ocurren en el ciberespacio, ¿existe un proceso de toma de decisión específico para las acciones de respuesta en el ciberespacio?

7. PERSONAL DE CIBERDEFENSA

7.1. ¿Existe personal específico para la ciberdefensa (nueva especialidad)? ¿Ha sido creado con una plantilla propia? ¿Existe una carrera autónoma en ciberdefensa?

7.2. El proceso de admisión y selección del personal para la ciberdefensa

7.2.1. ¿Es diferenciado?

7.2.2. ¿Tiene requisitos propios?

7.2.3. ¿Es realizada a nivel conjunto o en los ejércitos? ¿Cuál es el proceso?

7.2.4. Las nuevas generaciones (millennials o la generación Y) están especialmente capacitadas para trabajar en el ciberespacio, sin embargo, tienen dificultades para trabajar y operar en organizaciones con una fuerte componente jerárquica, como es el caso de las Fuerzas Armadas. ¿Qué respuesta dan a estos desafíos? ¿Utilizan nuevos modelos de incorporación?

7.2.5. ¿La estructura de ciberdefensa tiene operadores civiles? En caso afirmativo, ¿en qué nivel se encuentran? ¿Cuáles son sus misiones básicas?

8. INFRAESTRUCTURAS DE CIBERDEFENSA

8.1. ¿Cuáles son las infraestructuras donde se alojan las capacidades de defensa cibernética?

8.2. ¿Qué dependencia tienen?

8.3. ¿Pertenecen al nivel conjunto o a los ejércitos (tierra, mar y aire)?

9. PRESUPUESTO DE CIBERDEFENSA

9.1. ¿La defensa cibernética dispone de un presupuesto específico?

9.2. ¿Quién es la autoridad de gestión presupuestaria?

Apêndice E — Contributos para o conhecimento

1. Ciberdefesa ou defesa cibernética

1.1. Finalidade

Incorporar nas FA a capacidade de projetar força no, ou através do, ciberespaço, de modo a assegurar os mecanismos de proteção e defesa do estado, garantindo a liberdade de ação do estado e dos cidadãos.

1.2. Definição

Conjunto de atividades realizadas no ciberespaço com a finalidade de proteger os nossos sistemas de informação, obter dados para a produção de informações e para a preparação do ambiente operacional, e, quando justificado[53], atuar nos sistemas do oponente.

2. Estrutura do ciberespaço

A conceptualização das operações, à semelhança do que acontece nos restantes domínios, obedece à lógica da intenção e dos efeitos que pretendem atingir, concorrendo para o efeito a necessidade de entender o ciberespaço como teatro de operações. Considerando a caraterização efetuada do ciberespaço, releva a necessidade de proceder à sua estratificação em função dos elementos intrínsecos identificados, que são condicionadores da manobra, propondo-se a estratificação do ciberespaço em 5 camadas, conforme Figura 20. Sugere-se que o conceito de operações, nomeadamente a manobra (fogo e movimento) deve atender as três dimensões principais: cognitiva (centrada no homem), informacional[54] (centrada nos dados) e física (centrada no material).

[53] Termos específicos (autorização, procedimentos, ….) a definir.

[54] Sublinha-se que, como já acontece com a maioria de nós, uma pessoa pode ter várias ciber identidades, reforçando a dificuldade de atribuição de responsabilidades no ciberespaço.

Figura 20 – Estrutura do ciberespaço

Fonte: Adaptado de USJCS (2013)

3. Operações no ciberespaço

Em função da pesquisa e estudo efetuados, e não tendo merecido reparos por parte das entidades entrevistadas, CEMGFA (Monteiro, 2017) e ao CEM do CCOM (Cunha, 2017), parece fazer sentido, no caso nacional, entender a ciberdefesa como materializando a capacidade das FA conduzirem operações no ciberespaço, orientação, aliás, incorporada no objetivo geral deste trabalho.

3.1. Definição

Conjunto de processos que alterem intencionalmente um ou mais fatores do ciclo de vida dos elementos do ciberespaço.

3.2. Finalidade

Assegurar a liberdade de ação das nossas forças no ciberespaço, negar a liberdade de ação às forças adversárias ou oponentes, e apoiar ou potenciar outras atividades operacionais.

3.3. Espectro

Da literatura consultada e da informação apurada, considerando o quadro de riscos e ameaças e atendendo às missões atribuídas às FA no âmbito da ciberdefesa (Governo, 2015d, p. 5287), julga-se poder sistematizar o espectro de operações no ciberespaço conforme Figura 21.

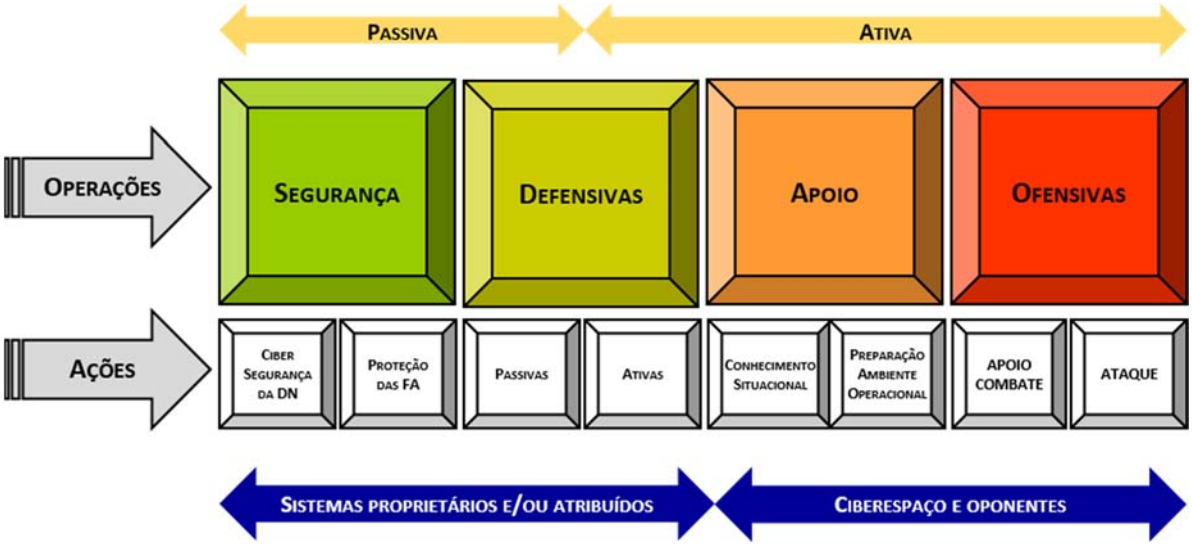


Figura 21 – Espectro de operações no ciberespaço

Fonte: Autor (2017)

3.4. Tipologia

- **Operações de segurança**

  Orientadas para a proteção dos sistemas proprietários ou atribuídos.

- **Operações defensivas**

  Orientadas para uma missão ou ameaça específica.

- **Operações de apoio**

  Orientadas para o conhecimento situacional[55] e para a preparação do ambiente operacional[56].

[55] Produção de informações.

[56] Planear e preparar as operações seguintes, podendo incluir: configurações de sistemas/redes ou estruturas físicas conectadas ou associadas (para incluir software, portas e intervalos de endereços de rede atribuídos ou outros identificadores), visando identificar vulnerabilidades dos sistemas adversários; ações tomadas para assegurar o acesso e controlo futuro dos sistemas/redes adversários.

- **Operações ofensivas**

  Orientadas para a projeção de força no/através do ciberespaço[57].

4. Organização da ciberdefesa

4.1. Nível estratégico e operacional

Comando de Operações no Ciberespaço (COC)[58] ou Comando do Ciberespaço (CC)[59], nas dependências hierárquica do CEMGFA, funcional do CCOM e técnica da DIRCSI, com a missão genérica de, enquanto CERT da DN, assegurar as responsabilidades da cibersegurança setorial, e, enquanto comando de componente, planear, integrar e dirigir as operações no ciberespaço.

Aspetos a considerar:

- Os comandos das componentes militares e os comandos operacionais dos ramos das FA devem ter a capacidade de integrarem as ações do COC através das suas capacidades específicas.
- O COC, como requisito operacional enquanto comando de componente, deve ter a capacidade de executar operações no ciberespaço, independentemente ou em coordenação com outras entidades no quadro de responsabilidades das FA na segurança do ciberespaço nacional (ENSC).

4.2. Nível dos estados-maiores

Implementação de células de ciberdefesa ou reformulação das **células J/G 6**, incorporando as valências ciber.

4.3. Nível tático

Implementação **capacidades específicas nos ramos**.

Criação de **módulos ciber**, ao nível do EMGFA, para apoio às operações conjuntas e ao emprego da Força de Reação Imediata.

---

[57] Elemento multiplicador do potencial de combate.
[58] Por absorção do Centro de Ciberdefesa.
[59] Na lógica das componentes naval e aérea (e Comando Naval e Comando Aéreo).

5. TTP

Dimensões	Contributos	Indicadores							
		Doutrina	Organização	Treino	Material	Liderança	Pessoal	Infraestruturas	Interoperabilidade
Pessoas	Novo paradigma de objetivos: **ambiente informacional** *versus* **ambiente operacional**.	●		●		●			
	Redes como plataforma de **operações** (condução da guerra) em detrimento da rede como plataforma de **serviços**.		●	●	●			●	●
	Implementação de requisitos da **ciber higiene**. Atualmente a maior parte das capacidades militares estão baseadas em TIC, cujo bom funcionamento (integridade, confidencialidade e disponibilidade) são vitais para o acesso, operação e manutenção destes sistemas. Por outro lado, não se pode esquecer a dimensão organizacional *pessoas* (indivíduos e ciber personas) e da sua crescente dependência, quotidiana, do uso das TIC e *social media*, que as torna vulneráveis às ações no ciberespaço que procuram manipular e/ou influenciar comportamentos, com sérios impactos organizacionais (funcionamento interno, credibilidade, pessoal das FA e famílias). Estender a estes elementos os requisitos de resiliência em cibersegurança.			●		●			
	A dinâmica e a complexidade do ciberespaço exigem uma adaptação contínua à envolvente operacional, colocando às FA o desafio adicional de recrutar e reter pessoal devidamente qualificado, ou a qualificar, capaz de integrar os requisitos inicialmente estabelecidos e, proativamente, promover a inovação e a evolução constante tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades.		●			●			
	Mudança da mentalidade das lideranças de modo a assimilarem a ciberdefesa como **multiplicador do potencial de combate**, promovendo a sua integração em todas as fases do planeamento das operações	●				●		●	●
	Parametrização do ambiente operacional em função de **objetivos intangíveis**, por contraponto aos tradicionais objetivos tangíveis (físicos).		●	●				●	
	Postura de **cibersoberania**.		●			●			
	Integração das capacidades cibernéticas nos diversos domínios das operações militares.	●	●	●	●	●		●	●
	Resistência à mudança: o papel das capacidades ciber na condução das operações.	●			●			●	
	Indivíduo *versus* ciber identidades: o **anonimato** e a dificuldade de atribuição de responsabilidades dos atos cometidos no ciberespaço.		●	●					
	Competências: necessidade de períodos de tempo prolongados para formação, treino e permanência em funções.		●	●		●			

Dimensões	Contributos	Indicadores							
		Doutrina	Organização	Treino	Material	Liderança	Pessoal	Infraestruturas	Interoperabilidade
Pessoas	**Partilha de informação** (*cyber intel*) entre os diversos atores/setores da segurança do ciberespaço, de modo a agilizar os processos e tornar mais eficiente as ações de **prevenção**, **mitigação**, **resposta**, **proteção** e **recuperação** de incidentes e/ou ataques cibernéticos.		●		●			●	●
	As características intrínsecas do ciberespaço, enquanto domínio de operações, inviabiliza o conceito de **supremacia** ou mesmo de superioridade prolongada no tempo.	●	●	●					
	Peopleware como novo elemento do ciclo de vida do ciberespaço.	●	●	●		●			
	Comunicação estratégica, a reafirmação do empenhamento nacional na proteção e salvaguarda da liberdade de ação de Portugal no espaço cibernético.		●			●		●	
Processos	Ciberespaço como **domínio defensável**.	●	●	●	●	●		●	
	As operações no ciberespaço nas guerras hibridas mais recentes, caracterizadas por uma utilização extensiva do ciberespaço para consecução de ciberataques, mas também como palco privilegiado para ações de propaganda e recrutamento.	●		●					
	Estabelecimento de **procedimentos** e **rotinas** para articulação entre o nível estratégico-operacional (COC) e o nível tático (*cyber work force*).		●	●		●	●	●	●
	Definição de **regras de empenhamento** relativamente à segurança do ciberespaço nacional (nomeadamente ao nível do CSSC).	●				●		●	●
	Um novo **ambiente operacional**: da *Internet of Things* (IoT), em que a comunicação é essencialmente entre equipamentos, *machine-to-machine* (M2M) para a *Internet of Everything* (IoE), em que a conexão inteligente é realizada entre pessoas, dados e equipamentos (numa 1ª fase no estágio *machine-to-people* (M2P) e numa 2ª fase *technology-assisted people-to-people* (P2P).	●	●	●	●	●		●	●
	Articulação entre as **operações de informação** e as **operações no ciberespaço**.	●		●		●			
	Integração sinérgica das capacidades de guerra cibernética e de **guerra eletrónica** (CW e EW) numa estrutura de direção que maximize a ação no espetro eletromagnético.	●		●		●			
	As operações ofensivas e a produção de **efeitos cinéticos** nos objetivos.	●		●	●	●		●	
	Necessidade de ajustar o ciclo das informações em função das caraterísticas do ciberespaço. A cibercapacidade como vetor privilegiado para o lançamento de ataques no contexto de **guerra híbrida**.	●		●			●		●
	Operações ofensivas centralizadas ao mais alto nível do processo da tomada da decisão.	●	●			●	●	●	

Dimensões	Contributos	Indicadores							
		Doutrina	Organização	Treino	Material	Liderança	Pessoal	Infraestruturas	Interoperabilidade
Processos	**Operações defensivas** distribuídas em toda a estrutura operacional.	●	●			●	●	●	
	Ciberespaço como denominador sinérgico do **multidomínio**, constituindo este o elemento chave para o sucesso das operações militares.	●			●				●
	Coordenação das diversas entidades com responsabilidade nas atividades de segurança do ciberespaço nacional, de modo a garantirem as adequadas ações de prevenção, mitigação, resposta, proteção e recuperação.		●	●				●	●
	Ciclo de aquisição de cibercapacidades é incompatível (dinâmica evolutiva da tecnologia do ciberespaço) com o tradicional ciclo de aquisição de material bélico.		●			●	●		
	Avaliação permanente da situação no ciberespaço que permita aos decisores e estados-maiores o tempo necessário para analisar, planear e executar as necessárias ações de resposta a ciber ameaças.		●			●		●	
	Ciberespaço como elemento potenciador da transição de **sistemas** de 4º para **5ª geração**, abrangendo plataformas com funções de fusão da informação e comunicação autónoma.	●	●	●	●	●	●	●	●
	Articular o processo de ***cyber intelligence*** entre as necessidades de informação e as atividades de **preparação do campo de batalha** (OPE).	●	●		●				
	Estabelecimento de níveis de decisão relativamente às ações/operações cibernéticas (político, estratégico, operacional e tático)		●	●		●	●		
	Definição do **ciberespaço de interesse nacional**, que concorra para a definição das capacidades cibernéticas a implementar nas Forças Armadas.	●			●			●	
	Definição do **nível da ameaça** que catalise as operações ofensivas no ciberespaço.	●			●	●			
	Aplicação do conceito ***constituency*** (conjunto de utilizadores, localização, TIC e organizações), em função de demarcações organizacionais, geográficas, políticas, técnicas ou contratuais.					●	●	●	
	Implementação de um **sistema de defesa em profundidade** que habilite a estrutura das FA, quando sob ataque, a sofrer uma degradação, ainda que progressiva, ao invés da sua destruição.	●	●			●	●	●	●
	Sistema de alerta de incidentes no ciberespaço			●	●			●	●

DIMENSÕES	CONTRIBUTOS	INDICADORES							
		Doutrina	Organização	Treino	Material	Liderança	Pessoal	Infraestruturas	Interoperabilidade
TECNOLOGIA	Implementação de requisitos de segurança simultaneamente nos equipamentos como na informação residente.			●	●	●	●		
	Consciência do **combate assimétrico**: para os ciberatacantes basta encontrar uma porta de entrada nos nossos sistemas (uma vulnerabilidade) e para as Forças Armadas a missão é garantir a defesa de todo perímetro (zero vulnerabilidades).		●	●		●	●		
	Comunicação estratégica, a reafirmação do empenhamento nacional na proteção e salvaguarda da liberdade de ação de Portugal no espaço cibernético.					●	●		
	O ciberespaço pode em determinado momento incluir ou não a internet, sendo esta abrangência voluntária, função da decisão humana, subsistindo outros aspetos do ciberespaço como as *intranets*, sistemas de armas e C2.				●		●		
	Os procedimentos de segurança no ciberespaço como responsabilidade partilhada por todos os escalões e níveis de decisão.					●	●		
	Integração das cibercapacidades com os sistemas de armas dos outros domínios.		●	●	●	●	●		
	Capacidade do **COC**, por crescimento, de integrar elementos do CSSC (estados de exceção e de guerra).		●	●	●		●		
	Implementação de **Módulos Operacionais de Ciberdefesa** (MOC) para apoio a operações (nível operacional-tático).		●	●	●			●	●
INFRAESTRUTURAS	Tecnologias adaptadas ao treino, privilegiando o uso intensivo de ***cyber ranges***.		●	●	●		●	●	
	Sistemas com capacidade de **fusão de dados**.				●		●	●	
	Incorporação de requisitos funcionais e técnicos baseados em **tecnologias *stealth***.	●		●	●		●	●	
	Inclusão de requisitos operacionais, funcionais e técnicos nos sistemas militares que assegurem a capacidade de **autodiagnóstico** e de **regeneração autónoma**.	●			●	●	●	●	
	Implementar mecanismos de interligação com as entidades do CSSC em função dos standards definidos pelo CNCS.				●			●	●
	Consciencialização do efeito ***momentum*** (grande impacto no objetivo) na utilização das armas cibernéticas (menor massa, mas maior velocidade, com custos muito reduzidos).	●		●		●	●		

Tabela 16 – TTP

Fonte: Autor (2017)